PC WELT SONDERHEFT
April/Mai/Juni 2007
www.tecChannel.de

200 Seiten plus CD

tecCHANNEL

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 10,90
Österreich € 12,00
Benelux € 12,55
Schweiz SFR 21,80

Netzwerk

- Tipps: Die besten Netzwerk-Tools
- IDS: Angriffe erkennen und abwehren
- Gruppenrichtlinien: Windows zentral managen
- Downtime: Das unterschätzte Risiko

E-Mail

- Domino: Domain Monitoring und Server-basierte Zertifikate
- DAMO: Outlook und Domino elegant kombiniert
- Spam-Schutz für Exchange

Wissen&Praxis

- 17 Linux-Distributionen für den Spezialeinsatz
- SOA-Grundlagen
- Novell Storage Services
- Oracle-Datenbank-Tuning
- Lancom 1823: Die Fritz!Box fürs Business
- Funknetze für die Gebäudeautomation

4 195914 910906 02

Editorial

Liebe Leser,

mit dieser Ausgabe begrüßen wir zum ersten Mal offiziell die Abonnenten der Experts-Inside-Heftreihe. tecCHANNEL hat im Februar die vier Inside-Hefte Lotus Domino/Notes, Windows NT/2000 Exchange, Netware/Novell sowie Access übernommen und wird sie thematisch online und „gedruckt" weiterführen.

Dies bedeutet für tecCHANNEL-Compact ein wesentlich umfangreicheres Themenspektrum, von dem sowohl die bisherigen Compact-Leser als auch die von Expert's Inside profitieren. Auch auf tecChannel.de werden Sie diese zusätzlichen Inhalte bemerken. Die bekannten Fachautoren von Expert's Inside verstärken dazu unser Autorenteam. Wir haben außerdem den kompletten Jahrgang 2006 von Expert's Inside in tecCHANNEL-Premium integriert und führen nicht nur die begonnenen Artikelserien dort nahtlos fort. Darüber hinaus haben wir das PDF-Archiv auf tecChannel.de um vier Jahrgänge von Expert's Inside erweitert – das sind mehr als 200 zusätzliche eBooks!

Diese tecCHANNEL-Compact-Ausgabe ist die erste, die thematisch erweitert wurde. Wir wollen bei der zukünftigen Planung nicht ohne Sie vorgehen. Nutzen Sie unsere Online-Leserbefragung, und teilen Sie uns mit, wie sich tecCHANNEL-Compact weiterentwickeln soll, damit es Ihre Anforderungen voll erfüllt.

Die Umfrage finden Sie bis Mitte April unter www.tecChannel.de/compact0207

Unter allen Teilnehmern verlosen wir als Dankeschön mehr als 50 wertvolle Fachbücher aus dem Pearson-Verlag.

Viel Spaß beim Lesen dieser Compact-Ausgabe wünscht Ihnen

Michael Eckert
Chefredakteur tecCHANNEL

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Stellv. Chefredakteur / CvD: Albert Lauchner
Grafik: stroemung, Michael Oliver Rupp, Bernd Maier-Leppla, Multimeda Schmiede
Titelgestaltung: Twentyfirst Communications

Redaktion tecCHANNEL:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897, Fax: -878
Homepage: www.tecChannel.de,
E-Mail: feedback@tecChannel.de

Autoren dieser Ausgabe: Jürgen Donauer, Mike Hartmann, Moritz Jäger, Martin Kuppinger, Ulrich Lenz, Klaus Manhart, Axel Sikora, Ramon Schwenk, Andreas Wurm
Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Business Media GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, vor allem durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags nicht zulässig.
Titelbild, CD-Cover: gsiCom, Helmut Payer
Anzeigen:
Anzeigenleitung: Dirk Limburg,
Tel.: 0 89/3 60 86-871
Leitung Anzeigendisposition: Rudolf Schuster,
Tel.: 0 89/3 60 86-135, Fax: -99 135
Digitale Anzeigenannahme:
Manfred Aumaier, Tel.: 0 89/3 60 86-602,
Andreas Mallin, Tel.: 0 89/3 60 86-603
Druck: Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen

Vertrieb / Produktion:
Gesamtvertriebsleitung: Josef Kreitmair
Vertriebsassistenz: Melanie Stahl
Vetriebsmarketing: Matthias Weber (Ltg.), Stefanie Kusseler, Ines Pariente
Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113,
E-Mail: mzv@mzv.de, Website: www.mzv.de
Produktionsleitung: Heinz Zimmermann
Jahresbezugs-Preise:
Inland: 39,20 EUR, Studenten: 34,80 EUR
Ausland: 42,20 EUR, Studenten: 37,80 EUR
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in tecCHANNEL-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA
Verlag: IDG Business Media GmbH, Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-0, Fax: -118,
Website: www.idg-verlag.de
Handelsregisternummer: HR 99187
Umsatzidentifikationsnummer: DE 811257800
Geschäftsführer: York von Heimburg
Verlagsleitung: Frank Klinkenberg
Vorstand: York von Heimburg, Keith Arnot, Pat Kenealy
Mitglieder der Konzerngeschäftsleitung:
Josef Lohner
Aufsichtsratsvorsitzender:
Patrick J. McGovern

Dieses tecCHANNEL-Compact wurde mit der Adobe Creative Suite CS produziert. tecCHANNEL-Compact erscheint im Verlag der PC-WELT. Zu unserer Verlagsgruppe gehören folgende Zeitschriften:

COMPUTERWOCHE · ChannelPartner · PC-WELT · DigitalWorld
Macwelt · GameStar · CIO · GamePro

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:
tecCHANNEL Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, Fax: (+49) 07 11/72 52-377, E-Mail: shop@tecchannel.de

Inhalt

	Editorial	**3**
	Impressum	**4**
1.	**Netzwerk**	**10**
1.1	**Lancom 1823, die Fritz!Box fürs Business**	**10**
1.1.1	Business-Lösungen	11
1.1.2	Lancom 1823 im Überblick	11
1.1.3	Im Praxiseinsatz	13
1.1.4	Installation	14
1.1.5	VPN-Server	15
1.1.6	VPN einrichten	16
1.1.7	Telefonie-Funktionen	17
1.1.8	Least Cost Routing	19
1.1.9	Eingehende Gespräche	20
1.1.10	Feature-Count	21
1.1.11	Fazit: Licht und Schatten	
1.2	**Funknetzwerke für die Gebäudeautomation**	**22**
1.2.1	Technische Einschränkungen	22
1.2.2	Grundsätzliche Neuerungen	23
1.2.3	Routing-Technologie	24
1.2.4	Produkte und Technologien	26
1.2.5	Die IEEE802.15-Arbeitsgruppe	26
1.2.6	Der ZigBee-Standard	27
1.2.7	Die Z-Wave-Technologie	28
1.2.8	EnOcean-Technologie im Detail	29
1.2.9	Fazit und Ausblick	30
1.3	**Überwachungssysteme in Netzwerken**	**31**
1.3.1	Funktionsweisen	31
1.3.2	Network-based Intrusion Detection System (NIDS)	32
1.3.3	Aufbau eines NDIS	32
1.3.4	Host-based Intrusion Detection (HIDS)	34
	CD-Inhalt	**35**
1.3.5	Network Node-based Intrusion Detection (NNIDS)	36
1.3.6	Wie wird ein Angreifer erkannt?	36
1.3.7	Erkennen von Missbrauch	37
1.3.8	Voraussetzungen	38
1.3.9	Suche nach Anomalien	38

1.3.10	Honeypots – Honigtöpfe für gierige Datendiebe	39
1.3.11	Angriffsabwehr mit Intrusion-Prevention-Systemen (IPS)	40
1.3.12	Verteidigungsszenarien mit IPS	41
1.4	**Networked Computing: Grundlagen und Anwendungen**	**42**
1.4.1	Cluster: Einsatzbereiche	42
1.4.2	Cluster: Das Grundprinzip	43
1.4.3	Cluster: Aufbau	43
1.4.4	Hochverfügbarkeits-Cluster	44
1.4.5	Einsatzgebiet und Verwaltung der HA-Cluster	45
1.4.6	Load Balancing und High Performance Cluster	46
1.4.7	Beowulf und Wolfpack	47
1.4.8	Beowulf Cluster	47
1.4.9	Grid Computing	48
1.4.10	Unterschiede: Cluster und Grid	49
1.4.11	Arten von Grids	50
1.4.12	Distributed Computing	52
1.4.13	Distributed Computing: Prinzip	53
1.4.14	Distributed Computing: Projekte	53
1.4.15	Peer-to-Peer-Netzwerke	54
1.4.16	Vor- und Nachteile von P2P	55
1.4.17	Collaboration	55
1.4.18	Fazit	56
1.5	**Netzwerk-Tools für kleine und mittlere Windows-LANs**	**58**
1.5.1	Packet Sniffing	58
1.5.2	Verbindungskontrolle	59
1.5.3	Administrationshelfer	61
1.5.4	Nützliche Tools	63
1.6	**Erste Hilfe nach dem Crash: Trinity Rescue Kit**	**65**
1.6.1	Grundsätzliches zur Distribution	65
1.6.2	Die Werkzeuge von TRK	66
	Die Virenscanner	66
	winpass und regedit	68
	NTFS-Partitionen mit CloneXP klonen	69
	mountallfs: Alle gefundenen Massenspeicher einbinden	70
	Ntfsundeleteall und photorec	71
	Datenserver mittels Samba	72
2.	**Linux / Novell Inside**	**75**
2.1	**QEMU-Puppy-Linux: Virtualisierung in der Hosentasche**	**75**
2.1.1	Herunterladen und Starten von QEMU-Puppy	76
2.1.2	Virtualisierung beschleunigen	77

2.1.3	Applikationen in QEMU-Puppy	78
2.1.4	Tipps und Tricks	79
2.1.5	Fazit	82
2.2	**17 Linux-Distributionen für den Spezialeinsatz**	**83**
2.2.1	BackTrack	84
2.2.2	Damn Small Linux und Damn Small Linux Not	84
2.2.3	Feather Linux	85
2.2.4	Fli4l und Coyote Linux	86
2.2.5	G4L (Ghost for Linux)	87
2.2.6	GeeXboX	87
2.2.7	GParted Livecd	88
2.2.8	grml	89
2.2.9	IPCop Firewall	90
2.2.10	Linux From Scratch	91
2.2.11	Linux LiveCD Router	91
2.2.12	Puppy Linux	92
2.2.13	SystemRescueCD	93
2.2.14	VideoLinux und Musix GNU+Linux	96
2.2.15	Fazit	97
2.3	**Novells Dateisystem unter Linux**	**98**
2.3.1	Wichtige Details zu den NSS und die Rolle von NCP	99
2.3.2	Die Partitionierung unter Linux	100
2.3.3	Pools und Volumes	101
2.3.4	NSS nutzen	102
2.3.5	Der NCP-Server	103
3.	**Grundlagen**	**105**
3.1	**Serviceorientierte Architekturen**	**105**
3.1.1	SOAs – Merkmale im Überblick	106
3.1.2	SOA-Dienste	107
3.1.3	Dienstverzeichnis und -nutzer	108
3.1.4	Ausführbare Aktionen	109
3.1.5	SOA – ein neues „Programmierkonzept“	110
3.1.6	SOA-Anwendungen	111
3.1.7	Enterprise Service Bus	112
3.1.8	Fazit	113
3.2	**Web Services – Grundlagen, Aufbau und Struktur**	**114**
3.2.1	Beispiele für Web Services	114
3.2.2	Merkmale von Web Services	115
3.2.3	Basiskomponenten von Web Services	117
3.2.4	Rollen und Aktionen	119

3.2.5	Web Services Stack – das Schichtenmodell	120
3.2.6	Nachrichten-, Service-, Ressourcen-, Richtlinien-Modell	121
3.3	**IT-Systeme: Ausfallsicherheit im Kostenvergleich**	**125**
3.3.1	Systemausfälle und ihre Folgen	125
3.3.2	Die Kosten des Stillstands	126
3.3.3	Systemausfall – das unterschätzte Risiko	127
3.3.4	Verfügbarkeit auf unterschiedlichem Niveau	127
3.3.5	Ausfallsichere Systeme im Kostenvergleich	128
3.3.6	Ausfallkosten im Vergleich	129
3.3.7	Fazit und Ausblick	131
3.4	**Oracle Datenbank-Tuning**	**132**
3.4.1	Datenbank Tuning	132
3.4.2	Performance-Planung	133
3.4.3	Optimierung von Instanz und Datenbank	135
3.4.4	Eine performante Datenbank erstellen	135
	Physische Objekte	135
	Segmente	136
	Hauptspeicher-Verwaltung	136
	Festplatten-Aktivitäten	137
	Verwaltung von Festplatten-Subsystemen	137
	Crash Recovery	138
	Statistiken sammeln	138
	Enterprise Manager	139
	Current State Views	140
	Counter/Accumulater Views	140
	Information Views	141
	Sonstige Views	142
4.	**Windows Server / Exchange Inside**	**144**
4.1	**Spam- und Virenabwehr mit Exchange**	**144**
4.4.1	So gelangen Spammer an Ihre Adresse	144
4.4.2	Offene SMTP-Relays	145
4.4.3	Blockieren bekannter Spammer	147
4.4.4	Echtzeit-Blockierlisten	149
4.4.5	Reverse-DNS-RBL-Dienste	151
	Reverse-DNS Beispiel	152
4.4.6	Verbindungsfilters für RDNS-RBL-Anbieter	152
4.4.7	Blockierung durch Challenge-Response	155
4.4.8	Signaturbasierte Filter	156
4.4.9	Hashbasierte Filter	157
4.4.10	Bayes-Filter	157
4.4.11	Randfilter	159

4.4.12	Speicherfilter	160
4.4.13	Clientfilter	160
4.2	**Windows-Management durch Gruppenrichtlinien**	**162**
4.2.1	Werkzeuge für das Gruppenrichtlinien-Management	162
4.2.2	Was man über Gruppenrichtlinien unbedingt wissen muss…	164
4.2.3	Vorsicht vor widersprüchlichen Richtlinien	164
4.2.4	Die Standardrichtlinien	165
4.2.5	Einige interessante Einstellungen	166
4.2.6	Gruppenrichtlinien und Systemversionen	168
4.3	**Sicherheitsmanagement im Active Directory**	**169**
4.3.1	Vordefinierte Gruppen	169
4.3.2	Weitere Gruppen	170
4.3.3	Die Delegation von Berechtigungen	171
4.3.4	Die vordefinierten Tasks	172
4.3.5	Benutzerdefinierte Tasks	173
4.3.6	Die Berechtigungen	174
4.3.7	Standorte und Dienste	176
5.	**Notes / Domino Inside**	**177**
5.1	**Domino: Der Server-basierte Zertifikatsdienst**	**177**
5.1.1	Basis der Zertifikate	177
5.1.2	Die Grundkonfiguration	178
5.1.3	Einstellungen zu Zertifikaten	179
5.1.4	Internet-Zertifikate	180
5.1.5	Weitere Funktionen	182
5.2	**Domino Domain Monitoring richtig nutzen**	**184**
5.2.1	Probes und Monitoring	184
5.2.2	Der Umgang mit Ereignissen	185
5.2.3	DDM Probes	186
5.2.4	Gezielte Analyse statt Unmengen von Daten	187
5.2.5	Eigene Probes erstellen	187
5.2.6	Hierarchien und Filter	188
5.3	**DAMO: Outlook und IBM Domino – elegant kombiniert**	**190**
5.3.1	Die Technologie hinter DAMO	191
5.3.2	Terminplanung und Kontaktverwaltung	192
5.3.3	Workshop: Installation von DAMO	193
5.3.4	Einrichten der Konten	194
	Glossar	**197**
	Index	**199**

1. Netzwerk

Netzwerke sind aufgrund neuer Technologien und den immer wichtiger werdenden Sicherheitsaspekten ein heiß diskutiertes Thema. In diesem Kapitel beschäftigen wir uns mit den im Tend liegenden VoIP Routern, die Voice over IP, ISDN und analoge Telefonie nahtlos integrieren. Außerdem geht es um die im Bereich Gebäudeautomatisierung konkurrierenden Funktechnologien. Gleich mehrere Hersteller ringen mit eigenen Funkstandards um Marktanteile.

Das Koppeln von Rechnern mittels Networked Computing und das Absichern von Unernehmensnetzen sind zwei weitere wichtige Aspekte der zunehmenden Vernetzung. Die Artikel zu Cluster-, Grid-, Peer-to-Peer- und Distributed Computing sowie zur Angriffsabwehr mittels Intrusion Detection beziehungsweise Intrusion Prevention (IDS/IPS) vermitteln nützliches Know-how. Für Administratoren stellen wir ausgewählte LAN-Tools vor, die den Verwaltungsaufwand bei der Netzwerkpflege minimieren sollen. Die meisten davon sind gratis und außerdem auf der Heft-CD zu diesem Compact enthalten. In die Werkzeugkiste von Systemverwaltern gehört außerdem die Linux-Live-CD Trinity Rescue Kit, die wir am Ende dieses Kapitels beschreiben. Damit lassen sich Rechner wiederbeleben, vergessene Windows-Passwörter zurücksetzen, der Netzwerkverkehr im Hintergrund überwachen oder PCs nach Viren scannen.

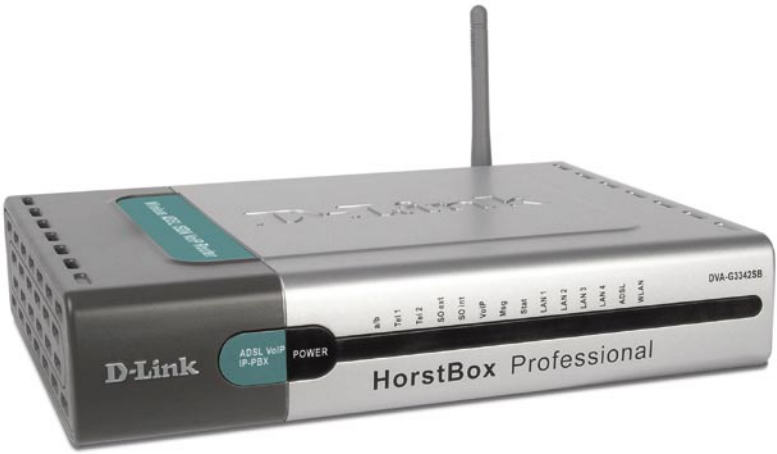
1.1 Lancom 1823, die Fritz!Box fürs Business

Eine der schwersten Aufgaben bei der Umstellung auf Voice over IP ist sicherlich die viel beschworene sanfte Migration. Es reicht nun mal nicht aus, mit dem Finger zu schnippsen und plötzlich ist VoIP in Unternehmensnetz und Telekommunikation integriert. Ziel einer Migrationsstrategie muss es sein, die bestehende Infrastruktur einzubinden und zunächst um VoIP zu erweitern. Die Erweiterung muss allerdings für den Benutzer unsichtbar und am besten ohne Funktionseinschränkung vonstatten gehen.

Für Home-User hat AVM diese Ziele mit der Fritz!Box sehr gut gelöst. Als Verbindung nach außen können ISDN, analog und VoIP zum Einsatz kommen, auf der lokalen Seite bietet das Gerät Anschluss für ISDN- oder analoge Telefone sowie mehrgerätefähige ISDN-Tk-Anlagen. Damit ermöglicht AVM es den Benutzern, wie bisher normal zu telefonieren und dennoch von den möglicherweise günstigeren VoIP-Tarifen zu profitieren. Für kleine und mittlere Firmen fehlt eine derartige Lösung zur Zeit noch, da hier die Anforderungen etwas höher sind. So müssen beispielsweise Außendienstmitarbeiter eingebunden oder mehrere Filialen vernetzt werden.

1.1.1 Business-Lösungen

Ein ähnliches Ziel haben sich mehrere Firmen gesteckt. So überraschte D-Link bereits Anfang 2006 mit der Mitteilung, unter dem Namen Horstbox Professional ein Gerät auf den Markt bringen zu wollen, das derartige Funktionen im Business-Umfeld bereitstellen soll. Allerdings ist die Horstbox immer noch nicht verfügbar. Ein Problem besteht wohl darin, dass die Horstbox auf einem Embedded Linux mit Asterisk als TK-Software aufsetzt. Die gesamte Integration musste also neu gemacht werden, da bisher noch kein D-Link-Produkt diesen Weg ging.



Horstbox: Die Hardware existiert schon, doch mit der Serienreife hapert es wohl noch, denn das Produkt ist immer noch nicht im Handel erhältlich.

Lancom dagegen verfügt mit LCOS schon seit ELSA-Zeiten über ein eigenes Betriebssystem mit ISDN- und Router-Funktionen. Dieses musste „nur noch“ um VoIP und einige andere notwendige Bestandteile erweitert werden, um den Lancom 1823 marktreif werden zu lassen. Zudem hat man sich offensichtlich mit der Ankündigung solange Zeit gelassen, bis man sicher war, das Gerät innerhalb einer definierten Zeitspanne fertig zu haben.

1.1.2 Lancom 1823 im Überblick

Das Gerät basiert auf einem Intel XScale iXP425 mit 533 MHz CPU-Takt, dem 32 MByte Speicher zur Verfügung stehen. WLAN steuert ein Atheros AR5414 bei, der Anwender hat die Wahl zwischen 802.11b/g (2,4 GHz) mit bis zu 108 MBit/s und a (5 GHz). Ein eingebautes ADSL-Modem sorgt für die Internet-Verbindung via ADSL2+. Zwei Ethernet-Ports lassen sich für LAN-Verbindungen nutzen oder

auch als WAN-Port konfigurieren, wenn der Internetzugang beispielsweise via SDSL- oder Kabelmodem erfolgt. Des weiteren stehen zwei analoge Anschlüsse für Endgeräte zur Verfügung und zwei für ISDN-Geräte oder -Anlagen. Einer davon lässt sich auch für einen analogen Amtsanschluss nutzen.

Standard-Design: Der Lancom 1823 kommt im Lancom-typischen Design daher.

Dicht gedrängt: Da Lancom kein größeres Gehäuseformat einführen wollte, reicht es nur für zwei Ethernet-Ports.

Die Vielfalt der Anschlussmöglichkeiten birgt auch ein nicht unerhebliches Fehlerpotential, das auch in der Zerstörung des Gerätes resultieren kann. Daher prangt auf der Anschlussleiste ein großer Warnaufkleber, dass man erst das Handbuch lesen möge, bevor man irgendwelche Geräte anschließt. Eine Kurzeinführung beschreibt die möglichen Varianten bei der Beschaltung der beiden ISDN-Anschlüsse und zeigt die gegebenenfalls zu setzenden DIP-Schalter. Hier stehen folgende

Möglichkeiten zur Auswahl:

- **ISDN 1:** analoger Amtanschluss, ISDN-Amtsanschluss (Basis oder S2m), Anschluss einer lokalen ISDN-Anlage oder von ISDN-Telefonen
- **ISDN 2:** Anschluss einer lokalen ISDN-Anlage oder von ISDN-Telefonen, ISDN-Amtsanschluss (Basis oder S2m)

Weitere Features

Der Router erlaubt die Einrichtung von bis zu acht logischen Funknetzen. Zur Absicherung kommen WEP, WPA oder WPA2 zum Einsatz. Diese Einstellung lässt sich für jedes WLAN getrennt vornehmen. Zudem kann das WLAN entweder direkt ins LAN integriert (Bridge) oder isoliert in einer DMZ betrieben werden. In diesem Fall müssen Pakete aus dem WLAN den Router und die Firewall passieren. Optional lässt sich auch eine VPN-Strecke (IPsec over WLAN) einrichten.

Der eingebaute Cron-Server kann zeitgesteuert Befehlssequenzen ausführen, beispielsweise um Verbindungen auf- oder abzubauen oder Konfigurationseinstellungen zu verändern. Damit das Gerät immer über die aktuelle Zeit verfügt, kann es sich mit einem NTP-Server oder über das ISDN-Netz synchronisieren. Gegenüber den Stationen im Netz kann der Lancom auch als NTP-Server auftreten.

Bestimmte Daten lassen sich als Feiertag einstellen, so dass diese Informationen anderen Systemkomponenten wie dem Cron-Server zur Verfügung steht. Sie müssen jedoch mühsam über ein benutzerunfreundliches Interface eingegeben werden. Wichtige Meldungen kann der Router über SNMP-Traps bereit stellen, via SYSLOG an einen Server schicken oder per SMTP an einen Mailserver übermitteln. Hierbei unterstützt er auch SMTP-Authentifizierung und SMTP after POP.

1.1.3 Im Praxiseinsatz

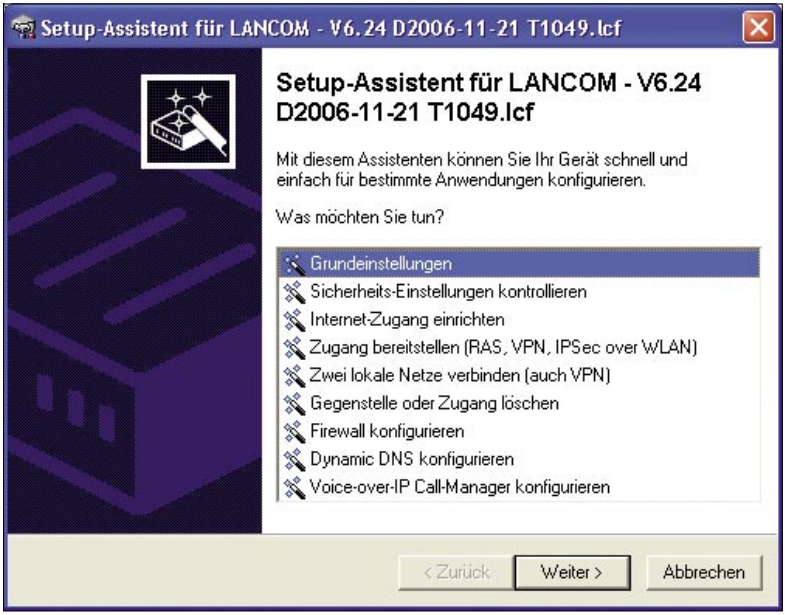
Für den Praxistest haben wir den Lancom 1823 wie folgt angeschlossen: Die Internet-Verbindung wird über QDSL-Home von QSC hergestellt. Da es sich hierbei nicht um ein echtes ADSL handelt, müssen wir das DSL-Modem am Ethernet-Port anschließen. An den verbleibenden Ethernet-Port hängen wir einen handelsüblichen Vier-Port-Switch. Das interne ADSL2+-Modem schalten wir ab. Der erste ISDN-Bus ist mit einem Telekom-ISDN-Anschluss verbunden, der zweite mit einem ISDN-Telefon. Die beiden analogen Ports bestücken wir jeweils mit einem DECT-Telefon. Ein Drucker am USB-Port vervollständigt den Aufbau.

Neben dem ISDN- und den analogen Telefonen sollen VoIP-Softphones zum Einsatz gebracht werden – eines im lokalen Netz und eines über Internet. Um letzteres zu realisieren, ist eine VPN-Strecke zwischen Client und Lancom 1823 einzurichten. Zusätzlich zum Telekom-Anschluss wollen wir über zwei SIP-Provider (sipgate.de und IPfonie von QSC) erreichbar sein. An den WLAN-Zugang stellen wir keine besonderen Anforderungen. Er wird über 802.11g mit WPA-PSK hergestellt und direkt ins LAN geleitet.

1.1.4 Installation

Nach Abschluss der Verkabelung geht es an die Einrichtung des Routers. Das Gerät lässt sich per Telnet/SSH, HTTP(S) und das mitgelieferte Tool LANconfig konfigurieren. Jede der drei Varianten hat ihre speziellen Vor- und Nachteile:

Bei **Telnet/SSH** hat man Zugriff auf alle Einstellungsmöglichkeiten, dafür ist die Handhabung mühselig und auf Hilfen muss man verzichten. Der **Web-**Zugriff präsentiert sich eher schlicht und bietet ebenfalls keine Hilfefunktionen. Dafür lassen sich einige Arbeitsschritte mit Hilfe von Wizards durchführen. Das nur für Windows verfügbare **LANconfig** bietet im Vergleich zur HTTP-Schnittstelle mehr Wizards und kann zudem eine Konfiguration auf mehrere Geräte übertragen. Dafür sind nicht alle Optionen konfigurierbar (etwa Zertifikate). Des weiteren ist auch dieses Programm nicht gerade ein Ausbund an Benutzerfreundlichkeit. Trotzdem greifen wir für die Erstinstallation auf LANconfig zurück.



Assistenten: Für eine Reihe von Aufgaben bietet das Konfigurationstool hilfreiche Wizards an.

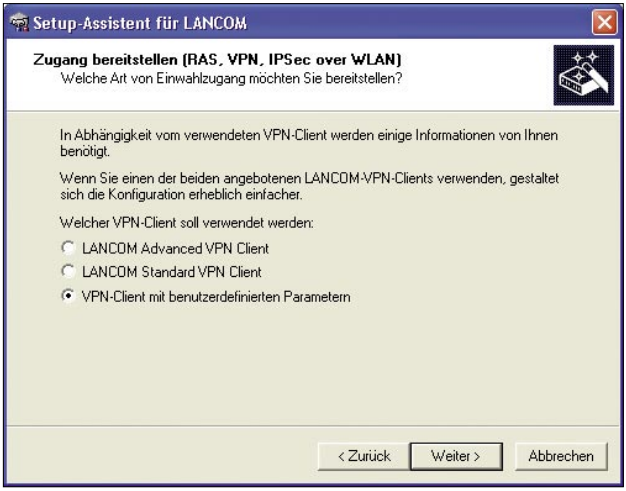
Zusätzlich bietet das Gerät SNMP und TFTP als Möglichkeiten. Diese werden primär für die Überwachungs-Tools und LANconfig genutzt. Für alle Varianten lässt sich für die verschiedenen Zugangsverfahren (Internet, LAN, WLAN) getrennt einstellen, ob der Zugriff generell, nur lesend oder nur via VPN erlaubt sein soll. Er lässt sich auch jeweils generell verbieten.

Mit Hilfe der Wizards sind die Grund- und Sicherheitseinstellungen, der Internet-Zugang sowie die grundlegenden Firewall-Regeln schnell erstellt. Für viele Situationen bietet das Programm sinnvolle Standardwerte an.

1.1.5 VPN-Server

Um ein VoIP-Softphone über das Internet einzubinden, benötigt man zunächst einen VPN-Tunnel, damit die Software über eine lokale IP-Adresse auf das Gateway zugreifen kann. Der Lancom 1823 verfügt über einen eingebauten VPN-Server, der in der Basisvariante maximal fünf gleichzeitige Verbindungen zulässt. Per Upgrade-Schlüssel lässt sich dieser Wert auf 25 aufbohren. Zudem schaltet der Schlüssel den VPN-Prozessor frei, so dass der Hauptprozessor weniger durch Ver- und Entschlüsselung belastet wird. Der Server kann auch mit VPN-Clients umgehen, die hinter einem NAT-Router stehen (NAT-Traversal).

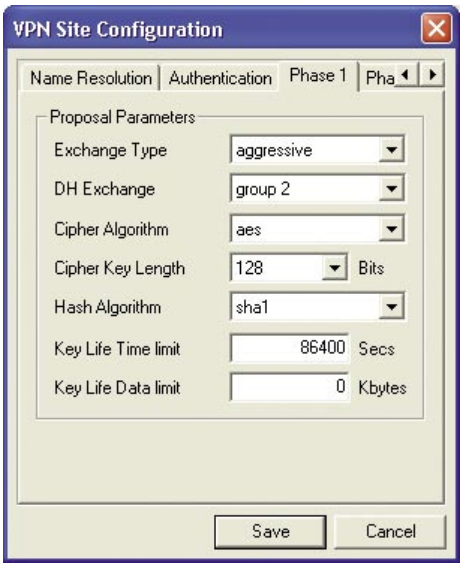
Bekanntermaßen ist die Einrichtung von IPSec-VPNs nicht trivial. Deshalb bietet Lancom auch für diese Aufgabe einen Wizard an. Nach dem Start wählt man aus, für welche Art von Client der Zugang einzurichten ist. Hier hat man die Auswahl zwischen „Lancom Advanced VPN Client“, „Lancom Standard VPN Client“ und „VPN-Client mit benutzerdefinierten Parametern. Bei ersterem handelt es sich eine OEM-Version des NCP-VPN-Clients, die für 109 Euro pro Lizenz zu kaufen ist. Den „Standard-Client“ hat Lancom inzwischen gar nicht mehr im Programm. Hierbei handelte es sich eigentlich nur um einen Wrapper um die IPSec-Implementation von Windows XP. Bei der dritten Option muss man sich schon gut mit IPSec-VPNs auskennen, um unfallfrei eine Verbindung einzurichten.



Nicht mehr ganz aktuell: Den „Standard Client“ gibt es nicht mehr.

1.1.6 VPN einrichten

Leider ist die Dokumentation zur VPN-Einrichtung sehr dürftig. Denn aus der Aussage „Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein“ lässt sich nur wenig Hilfe ziehen. Auch die Verwendung von Schlüsseldateien ist nicht beschrieben, außer dem Hinweis, dass man Schlüssel über die HTTP-Konfigurationswebseite hochladen kann. Hier wäre ein praxisnäheres Handbuch mehr als wünschenswert. Insbesondere eine Anleitung, wie man zumindest den Windows-VPN-Client anbindet.



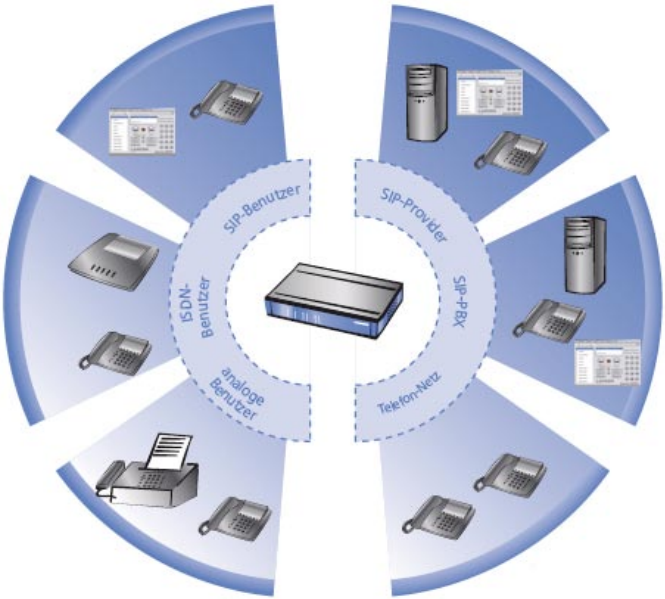
Freeware: Anstatt des kostenpflichtigen Advanced VPN Client kann man auch auf die Freeware von Shrew zurückgreifen.

Wenn gar nichts mehr hilft, bleibt zumindest ein Blick in das von Benutzern betriebene lancom-forum (www.lancom-forum.de). Hier haben wir auch den Hinweis auf den Freeware-VPN-Client von Shrew Soft (www.shrew.net) gefunden. Mit diesem gestaltet sich die Einrichtung einer VPN-Verbindung vergleichsweise einfach. Zwar nicht ganz so einfach wie mit dem Advanced Client, dafür allerdings kostenlos.

1.1.7 Telefonie-Funktionen

Neben den von Lancom-Produkten hinlänglich bekannten Router- und Sicherheitsfunktionen geht es beim 1823 primär um die Integration von VoIP, ISDN und analoger Telefonie. Das Gerät kann alle drei Verfahren sowohl nach außen hin als

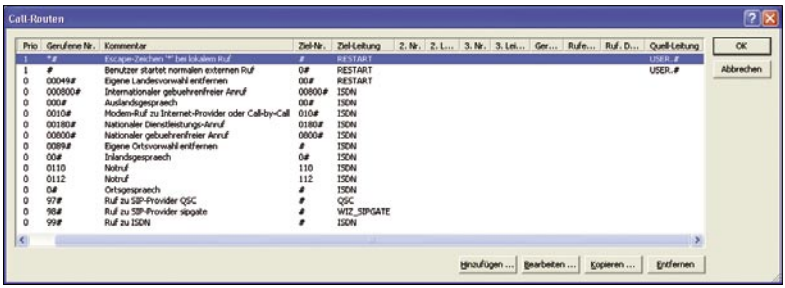
„Amts“-Leitungen als auch intern für Endgeräte bedienen. Herzstück ist der „VoIP Call Manager“, der zwischen den Verfahren vermittelt und bei Bedarf umkodiert. Der Call Manager unterscheidet zwischen Benutzern und Leitungen. Bei ersteren handelt es sich um Endgeräte wie analoge, ISDN-, oder VoIP-Telefone. Unter letzteren versteht der Call Manager Verbindungen nach außen, etwa einen ISDN- oder analogen Anschluss, sowie VoIP-Provider oder übergeordnete TK-Anlagen.



Telefonie im Überblick: Links die lokalen Anschlüsse, rechts die Verbindungen nach außen und in der Mitte der Lancom 1823. (Quelle: Lancom)

Auch für die Einrichtung der Telefoniefunktionen bietet Lancom einen Assistenten, der die wichtigsten Informationen wie MSNs oder SIP-Provider abfragt und lokalen Anschlüsse genutzt werden sollen. Daraus erstellt der Assistent die notwendigen Einträge in der Konfiguration und die Call-Routen. Diese legen fest, wie gewählte Telefonnummern umgesetzt werden und im Falle von ausgehenden Gesprächen, über welche Provider sie abgewickelt werden.

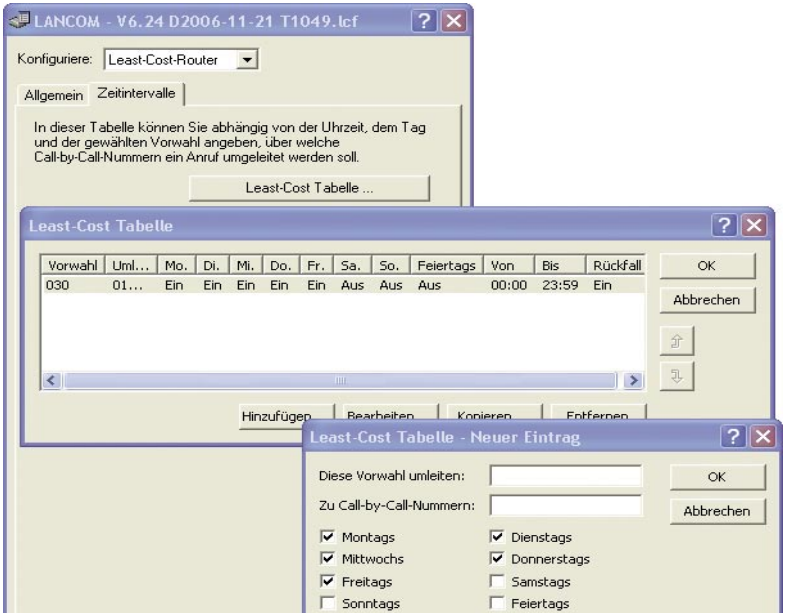
Die Verarbeitung kann abhängig vom lokalen Benutzer erfolgen und gegebenenfalls auch Anrufe verweigern, um beispielsweise gebührenpflichtige Vorwahlen zu sperren. Für den lokalen Benutzer ist es komplett transparent, über welche Leitung (ISDN oder SIP) ein Gespräch geführt wird. Er wählt einfach die gewünschte Rufnummer. Der Assistent konfiguriert die Call-Route aber so, dass der Benutzer durch Vorwahl einer speziellen Nummer, die Leitung dediziert auswählen kann.



Beliebig komplex: Über Call-Routen legen Sie fest, was mit ausgehenden Anrufen geschieht.

1.1.8 Least Cost Routing

Zwar findet sich in LANconfig auch der Punkt „Least-Cost-Router“, doch bezieht sich dieser lediglich auf ISDN-Einwahlverbindungen ins Internet und auf Clients, die per LANCAPI telefonieren oder faxen. Im Lancom-Forum finden sich einige Hinweise, wie man über den eingebauten CRON-Daemon die Call-Routing-Tabelle patchen kann, so dass eine Art LCR entsteht.



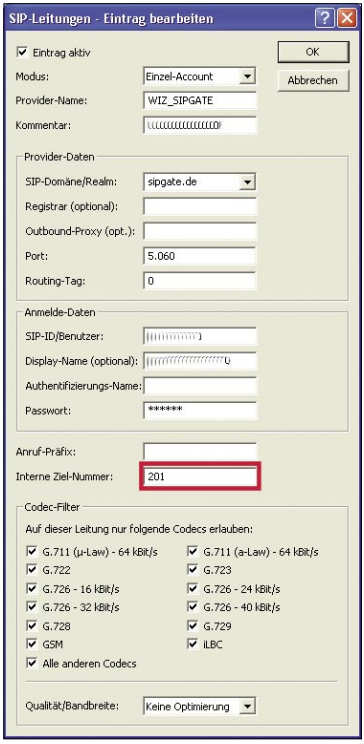
Eingeschränkt: Der Least Cost Router dient nur für LANCAPI- und ISDN-Einwählverbindungen nicht jedoch für den Call Manager.

Allerdings steht der Verwaltungs- und Programmieraufwand in keinem Verhältnis zu den möglicherweise zu erzielenden Einsparungen. Dazu kommt noch, dass ein stündliches Umschreiben der Konfiguration die Lebensdauer des Flash-ROM erheblich verkürzt. Zumindest dieses Problem kann man mit dem Befehl flash 0 auf der Telnet/SSH-Konsole umgehen. Dabei werden Konfigurationsänderungen nur im Hauptspeicher des Geräts abgelegt. Nach einem Reboot sind sie verloren.

1.1.9 Eingehende Gespräche

Abgesehen von der fehlenden Möglichkeit für einfaches Least Cost Routing sind die Optionen bei ausgehenden Gesprächen mehr als ausreichend. Bei eingehenden Gesprächen sind sie dagegen nicht ganz so üppig.

Fest zugeordnet: Eingehenden Leitungen muss derzeit noch ein lokaler Teilnehmer direkt zugeordnet werden.



So ist beispielsweise für jede Eingangsleitung ein internes Gerät als Gesprächsziel zu konfigurieren. Weitergehende Optionen wie Gruppenruf, Weiterleitungen bei Besetzt, nach einer bestimmten Zeit oder abhängig von Datum und Uhrzeit sind

derzeit nicht möglich. Auch fehlt die Möglichkeit, Aktionen von einem Telefon aus anzusteuern, wie es beispielsweise bei der Fritz!Box der Fall ist. Hier hat Lancom noch einiges nachzubessern.

Eingeloggt: Über VPN kann der Roadwarrior telefonieren als säße er im Büro.

1.1.10 Feature-Count

Auf der Haben-Seite kann der Lancom allerdings auch einiges für sich verbuchen. So unterstützt er eine Reihe von Codecs (G.711 a und u, G.722, G.723, G.726 mit 16/24/32/40 KBit, G.728, G.729, GSM und iLBC). Eine Wandlung findet nur statt, wenn es tatsächlich notwendig ist. Zur Bandbreitensteuerung bietet er reservierte Bandbreite, Traffic Shaping, Auswertung des DiffServ/TOS-Felds, 802.1p sowie automatische Anpassung der Paketgrößen.

Es lassen sich bis zu 40 lokale ISDN-Benutzer und 32 SIP-Endgeräte einrichten. Neben ISDN- oder analogem Amtsanschluss kann sich der Lancom 1823 mit vier SIP-TK-Anlagen verbinden und 16 Accounts bei SIP-Providern ansteuern. Dabei unterstützt der Lancom verschiedene Betriebsmodi:

Als Einzel-Account konfiguriert, bedient der Call-Manager eine einzelne VoIP-Rufnummer, die eingehende Anrufe an einen lokalen Benutzer weiterleitet. Im Trunk-Modus wird eine Stammrufnummer bedient, die letzten Stellen der gewählten Nummer verwendet das Gerät zur Identifizierung des lokalen Anschlusses. Als Gateway stellt der Router für eine entfernte SIP-TK-Anlage einen Übergang in ein lokales ISDN-Netz her. Das SIP-Gateway wird mit einer einzigen Nummer bei der SIP-TK-Anlage registriert, es sind allerdings mehrere Gespräche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite).

1.1.11 Fazit: Licht und Schatten

Man merkt dem Router an, dass er von einem Netzwerk-Spezialisten stammt. Hinsichtlich der Netzwerk- und Sicherheitsfunktionen lässt er kaum Wünsche offen, abgesehen vielleicht von einer etwas weniger mühsam zu bedienenden Konfigurationsoberfläche. Auf der TK-Seite hinterlässt er allerdings gemischte Gefühle. Zum einen ist da die nahtlose Integration der Telefoniemedien VoIP, ISDN und Analog. Zum anderen besteht hinsichtlich der Funktionen noch viel Spielraum nach oben. Dazu gehören sicherlich echtes Least-Cost-Routing für Telefonie, Einbindung der LANCAPI-Clients in den Call Manager, eine Reihe von TK-Funktionen und zusätzliche Möglichkeiten für den USB-Port. Auch wenn die Fritz!Box und der Lancom 1823 in zwei verschiedenen Ligen spielen und nicht wirklich vergleichbar sind: AVM hat bei den Funktionen einige Standards gesetzt, die als Messlatte dienen.

Betrachtet man allerdings die Update-Frequenz des hauseigenen Betriebssystems LCOS, kann man davon ausgehen, dass in nicht allzu ferner Zukunft noch viele Funktionen nachgereicht werden. Bei einem Preis von rund 600 Euro bietet das Gerät einen soliden Einstieg in die VoIP-Telefonie, ohne der neuen Technologie gleich auf Gedeih und Verderb ausgeliefert zu sein.

Wer mehrere Außendienstmitarbeiter per VPN und VoIP einbinden will, sollte die VPN-Option gleich mit einplanen. Nicht wegen der zusätzlichen Tunnel, sondern vor allem weil dadurch der VPN-Prozessor frei geschaltet wird. Dadurch bleibt mehr Rechenleistung für die VoIP-Kanäle.

Mike Hartmann

tecCHANNEL-Links zum Thema	Webcode	Compact
Lancom 1823, die Fritz!Box fürs Business	456438	S.10
Tuning und Hacks für die Fritz!Box	432803	–
Spezielle Sicherheitsaspekte bei VoIP im WLAN	437631	–
Bedrohungsanalyse beim Einsatz von VoIP-Systemen	437414	–
Workshop: Asterisk – mehr als VoIP	432904	–
VoIP hinter einer NAT-Firewall	433069	–
Stromversorgung und Kühlung für VoIP	432161	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

1.2 Funknetzwerke für die Gebäudeautomation

Funkbasierte Anwendungen sind für den Gebäudebereich keine Neuigkeit. Ausgehend von der Infrarot-Fernsteuerung für den Fernseher und dem funkbasierten Garagentoröffner gibt es mittlerweile eine Vielzahl von ferngesteuerten Anwendungen im Bereich der Hausautomatisierung (Home Automation). Diese reichen von der Alarmanlage, über die Heizungs-, Rolladen-, Steckdosen- und Lichtsteuerung bis hin zur Zählerfernauslesung auch von außerhalb der Wohneinheit.

In den letzten Jahren und Monaten sind eine Menge neuer Funktechnologien entwickelt worden, die nun auf den Markt drängen und versuchen, mit technischen Neuerungen einen Ausweg aus dem Wirrwarr von unterschiedlichen Funkstandards herbeizuführen. Dieser Beitrag betrachtet die grundsätzlichen Entwicklungen und stellt die wichtigsten Technologien vor.

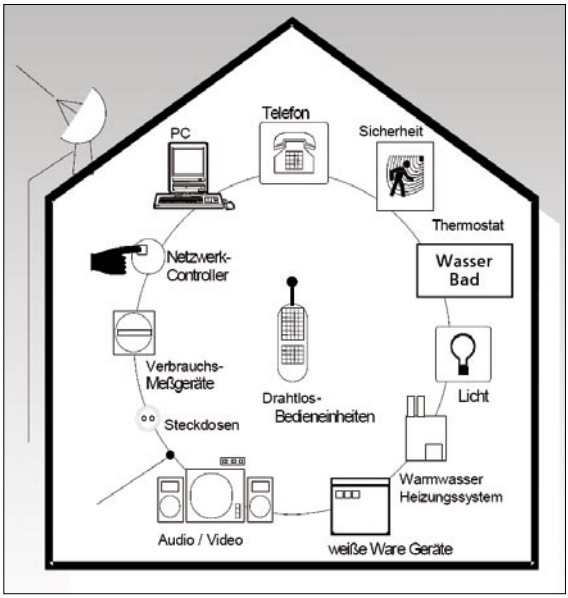
1.2.1 Technische Einschränkungen

Für die meisten Funknetzwerke im Gebäudebereich, die bis heute erhältlich waren, gelten einige einschränkende Aspekte. Diese müssen bei der Konzeption solcher Systeme berücksichtigt werden. Beim größten Teil der Funklösungen handelt es sich um Punkt-zu-Punkt-Systeme, die keinerlei Netzwerkfunktionalität erlauben. Bestenfalls sind noch sternförmige Netzwerktopologien zu finden, bei denen mit einer Fernbedienung mehrere Geräte angesteuert werden können. Ebenso sind die meisten Systeme herstellerspezifisch. Dies bedeutet, dass ein Gerät eines Herstellers nur mit der Fernbedienung desselben Herstellers bedient werden kann.

Viele der Systeme arbeiten nur unidirektional. Das heißt, dass die Daten lediglich in eine Richtung übertragen werden können, also von einem Sender zu einem Empfänger. Ein Funksystem kann aber nur dann zuverlässig arbeiten, wenn der erfolgreiche Empfang einer Information entsprechend quittiert wird. Hierzu sind bidirektionale Systeme notwendig. In der Praxis erhöht man die Wahrscheinlichkeit einer erfolgreichen Übertragung oft dadurch, dass der Datenrahmen mehrfach übertragen wird. Darüber hinaus kann man in den vielen herkömmlichen Fällen, in denen ein Mensch das Ergebnis unmittelbar überwachen kann, mit einer gewissen Unzuverlässigkeit leben. Hat sich zum Beispiel das Garagentor nicht geöffnet, dann wird der Knopf halt noch mal gedrückt.

Die meisten Systeme sind funktechnisch einfach gehalten, bestehen oft noch aus diskreten Schaltkreisen und haben einen hohen Platzbedarf. Ein „intelligenter" Datenaustausch ist mit solchen antiquierten Geräten meist nicht möglich. Funknetzwerke im Gebäudebereich arbeiten überwiegend auf Frequenzen in den unteren ISM-Bändern (Industrial-Scientific-Medical) – in Europa insbesondere in den Bändern bei 433 und 868 MHz. Da sich hier eine Vielzahl von Geräten tummeln, sind je nach technischer Ausführung Störungen nicht auszuschließen.

Zusätzlich muss konstatiert werden, dass der gesamte Markt der Gebäudeautomatisierung in den vergangenen Jahren deutlich hinter den Erwartungen zurückgeblieben ist. Alle Entwicklungen in Richtung intelligentes Haus, wie zum Beispiel das InHouse des Duisburger Fraunhofer Instituts IMS (www.inhaus-zentrum.de), haben zwar die technische Realisierbarkeit gezeigt, aber dennoch nicht die erhoffte und auch nicht die notwendige Marktdurchdringung erhalten. Grund: Es fehlen die herstellerübergreifende und die Wertschöpfungskette umfassende Durchgängigkeit ebenso wie die Marktakzeptanz.



Verständigungsprobleme: Es gibt mittlerweile im Hausbereich eine Vielzahl von Anwendungen, die per Funk angesteuert wurden. Allerdings bestehen diese Lösungen meist aus proprietären und ge-trennten Funksystemen. (Quelle: Fraunhofer Gesellschaft)

1.2.2 Grundsätzliche Neuerungen

Trotz gewisser technischer Einschränkungen der Funknetze im Gebäudebereich sind bei den Neuentwicklungen der letzten Jahre wesentliche qualitative und technische Veränderungen feststellbar.

Neben den einfachen Netzwerktopologien kommen in zunehmendem Maße nun auch vermaschte und Multi-Hop-Topologien zum Einsatz. Unter Vermaschung (Meshing) versteht man im Zusammenhang mit Funknetzen die Fähigkeit, dass ein Gerät mit allen Geräten, die sich in seiner Umgebung befinden, unmittelbar kommunizieren kann. Mit einer Multi-Hop-Fähigkeit hat ein Gerät die Möglichkeit, zwischen zwei Endknoten auch dann zu kommunizieren, wenn keine unmittelbare Funkverbindung existiert. Dann muss der Datenverkehr von anderen Zwi-

schenknoten weitergeleitet werden. Für eine solche Funktionalität sind dann Repeater- oder Routerkonzepte nötig. So ein Funknetzdesign beinhaltet einen wesentlichen Mehrwert, ist aber auch mit einem deutlichen Anstieg der Komplexität und Kosten verbunden.

Allerdings sind Multi-Hop-Topologien nur mit bidirektionalen Systemen sinnvoll nutzbar, da damit eine „intelligente" Kommunikation zwischen den Geräten möglich ist. Zusätzlich kann durch die Nutzung von Empfangsbestätigungen (Acknowledgements), wie sie ja auch bei WLAN vorgesehen sind, die Zuverlässigkeit von Datentransfers zwischen den Funksystemen deutlich erhöht werden.

Auf die Interoperabilität der unterschiedlichen Systeme wird immer größere Aufmerksamkeit gelegt. Dies setzt nicht nur identische Funkschnittstellen, sondern auch identische Anwendungsprotokolle voraus. Die Standardisierung solcher Funksysteme gewinnt somit eine immer größere Bedeutung. Zusätzlich spielt die Zuverlässigkeit insbesondere bei den Systemen eine große Rolle, bei denen Funknoten ohne menschliche Interaktion miteinander kommunizieren (Machine-to-Machine-Communication).

Immer mehr monolithisch integrierte Funkchips (RF-Transceiver) sind kostengünstig verfügbar. Neben der geringeren Stromaufnahme und dem geringeren Formfaktor erlauben sie in der Regel auch eine deutliche Reduzierung der Gesamtkosten. Solche Transceiver sind mittlerweile auch in Standardtechnologien für immer höhere Frequenzen verfügbar. Insbesondere können heute 2,4-GHz-Funksysteme kostengünstig integriert werden. Hierdurch stehen immer größere Bandbreiten für den drahtlosen Datenaustausch im Gebäudebereich zur Verfügung.

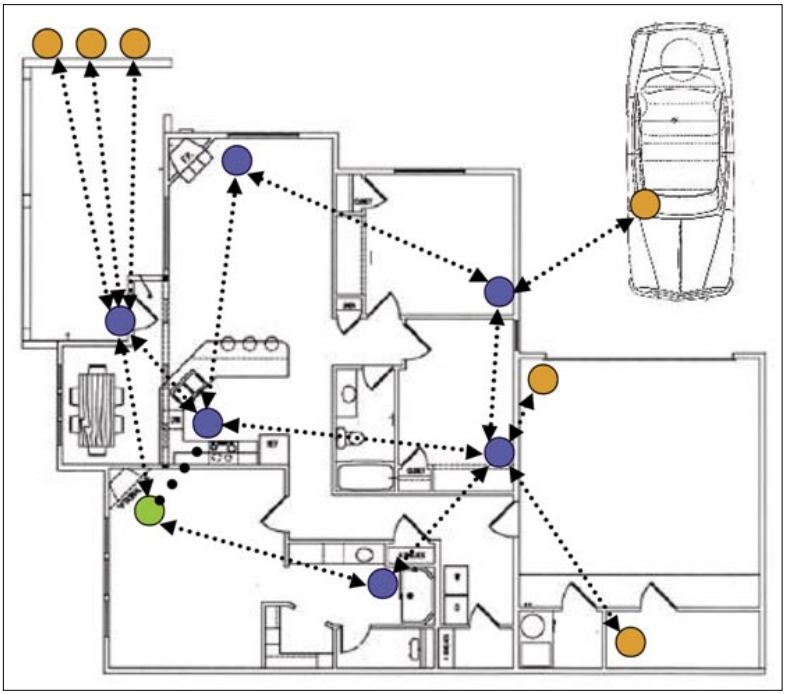
Schließlich und endlich – und das wurde bei den vorherigen Aspekten ja auch immer wieder angesprochen – lassen sich mit modernen, hochintegrierten Schaltkreisen sehr kostengünstige Systeme aufbauen. Und so gilt hier ebenfalls die banale Grundregel, dass eine Technologie in umso mehr Anwendungen Eingang findet, je günstiger sie realisiert werden kann.

1.2.3 Routing-Technologie

Die Weiterleitung der Daten Mit Hilfe von Repeatern oder Routern ist ein wesentliches Element für den umfassenden Einsatz von Funknetzen. Das bezieht sich nicht nur auf den Gebäudebereich, sondern auch besonders auf die Anwendungen der Industrie- und Gebäudeautomation.

Zum einen kann die wirksame Reichweite der Systeme deutlich erhöht werden. Dies ist umso wichtiger, je höher die Arbeitsfrequenzen der Systeme sind. Denn die Ausbreitungscharakteristik, vor allem im so genannten Indoor-Bereich, verschlechtert sich mit höheren Frequenzen bei gleichen Sendeleistungen zunehmend. Und bereits heute ärgert man sich oft genug darüber, dass die Reichweite der Sender durch Wände und besonders Stahlbetondecken deutlich begrenzt wird.

Zum anderen kann man mit Hilfe von autonomen Routing-Algorithmen auch die Zuverlässigkeit der Funksysteme erhöhen. Steht eine Funkstrecke oder ein Zwischenknoten nicht mehr zur Verfügung, kann das Datenpaket den Zielknoten auch über einen alternativen Pfad erreichen. Dies gilt auch dann, wenn der direkte Pfad nicht mehr zur Verfügung steht. Die aus ganz einfachen Funksystemen bekannten Repeater-Konzepte, die ungerichtet den Verkehr weiterleiten, sind nur für sehr kleine Netze realistisch, da der Verkehr im Netz exponentiell mit der Anzahl der Repeater zunimmt.



Automatische Navigation: Die autonome Wegefindung von Datenrahmen kann die Reichweite und die Zuverlässigkeit eines Funksystems wesentlich erhöhen. (Quelle: Texas Instruments)

Die Entwicklung leistungsfähiger Routing-Algorithmen und -Protokolle ist bereits seit Jahren ein Thema für die Forschung und Entwicklung. Vor dem Hintergrund der immer wieder unterschiedlichen Anwendungsanforderungen in Bezug auf Echtzeitverhalten, Grad der Gerätekopplung, Dynamik des Netzes, Zuverlässigkeit und Sicherheit stellen die Hersteller fest, dass für kostenoptimierte Systeme die Entwicklung neuer Verfahren sinnvoll und notwendig ist.

1.2.4 Produkte und Technologien

Die großen Halbleiter- und Systemhersteller haben den wachsenden und zukunftsträchtigen Markt längst erkannt und versuchen, sich rechtzeitig in Position zu bringen. Dies führt auch zu immer mehr unterschiedlichen Technologieansätzen und zu einem insgesamt recht unübersichtlichen Marktgeschehen.

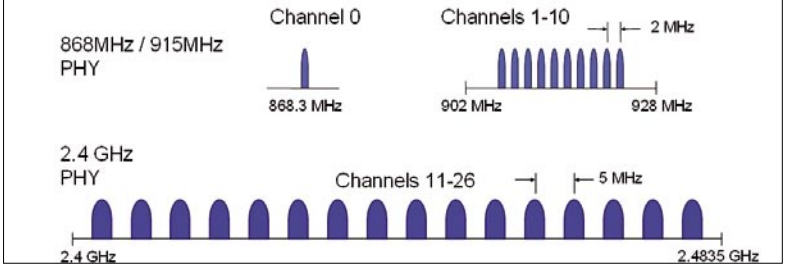
Leider ist dies – bezogen auf den gesamten Markt – eher kontraproduktiv, da die angestrebte Vereinheitlichung der Netze und die damit erreichbaren Stückzahlen für die gesamten Technologien so nicht erreicht werden können.

Die folgenden Abschnitte stellen drei wichtige Marktteilnehmer vor, die ihrerseits sehr unterschiedliche Produkt- und Technologieansätze verfolgen. Das sind im Einzelnen ZigBee, Z-Wave und EnOcean. Eines haben alle diese Technologien gemeinsam: Sie bauen auf den allgemeinen Standard IEEE805.15 auf.

1.2.5 Die IEEE802.15-Arbeitsgruppe

Die Arbeitsgruppe 802.15 kümmert sich im Allgemeinen um Wireless Personal Area Networks (WPAN), die Projektgruppe 4 um Low-Rate Wireless PANs. Die Basisversion des IEEE802.15.4 wurde im Oktober 2003 verabschiedet und steht auf der IEEE802.org-Homepage unter http://www.ieee802.org/15/pub/TG4b.html zum Download zur Verfügung. Er hat sich als übergreifender Standard herausgestellt, der auf außerordentlich große Akzeptanz stößt und auf den zahlreiche Protokolle auf der Netzwerk-, Transport- und Anwendungsebene aufbauen.

	channel assignment			data parameters			spreading parameters	
	frequency band	region	# of channels	data rate	symbol rate	symbols	chip rate	modulation
868/ 915 MHz	868 - 868,6 MHz	Europe	0	20 kbps	20 kBaud	binär	300 kchips/s	BPSK
	902 - 928 MHz	America	1-10	40 kbps	40 kBaud	binär	600 kchips/s	BPSK
2,4 GHz	2400 - 2483,5 MHz	worldwide	11-26	250 kbps	62,5 kBaud	16 orthogonal	2000 kchips/s	O-QPSK

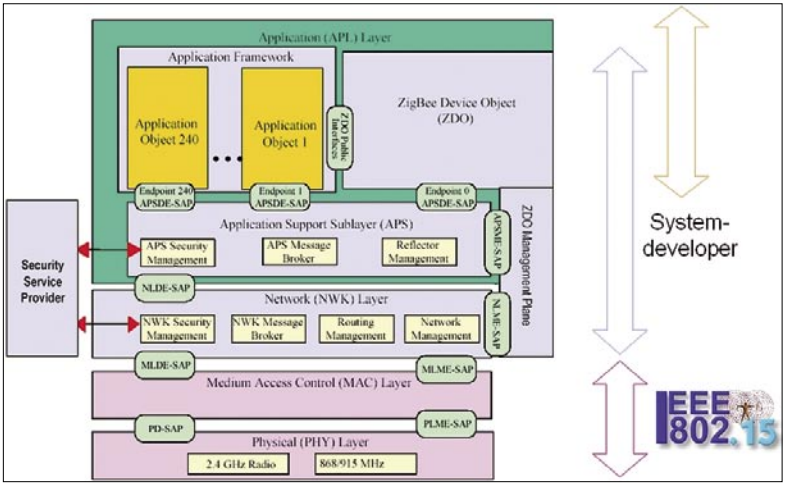


Grundlagen: Der IEEE802.15.4-Standard sieht die Übertragung von Daten entweder in den Sub-GHz-ISM-Bändern bei 868 beziehungsweise 915 MHz oder im 2,4-GHz-Band mit bis zu 250 kBit/s vor. Er nutzt ein DSSS-basiertes Frequenzspreizverfahren, um insbesondere die Probleme, die sich aus der Mehrwegeausbreitung der Funkwellen ergeben, zu verringern.

In zwei anderen Arbeitsgruppen, 802.15.4a und 802.15.4b, werden gegenwärtig weitere Features aus dem Bereich der Sicherheit und des Netzwerkmanagements und auch zusätzliche physische Übertragungsmechanismen erarbeitet. Hier reichen die unterschiedlichen Entwicklungsrichtungen von höheren Bandbreiten im Sub-Gigahertz-Bereich über Chirp Spread Spectrum (CSS) bis hin zu Ultra-Wide-Band-(UWB)-Ansätzen.

1.2.6 Der ZigBee-Standard

Die „ZigBee-Technologie“ ist aus den Aktivitäten um den gescheiterten WLAN-Wettbewerber HomeRF hervorgegangen und seit 2001 in der IEEE-Arbeitsgruppe 802.15.4 beziehungsweise seit 2002 in der ZigBee-Alliance (www.zigbee.org/en/) aktiv. Die ZigBee-Alliance ist im Bereich der Short Range Wireless Networks weiterhin die Vereinigung, die das größte Interesse und die größte Community auf sich vereinigt. An vielen Stellen wird der Begriff ZigBee als Synonym für diese Netze verwendet. Der Name ZigBee leitet sich übrigens ab von dem Zickzack-Tanz der Biene, die auf diese Weise ihren Artgenossen den Weg zur nächsten Nahrungsquelle mitteilt. Auf ähnliche Weise werden die Daten dann durch das Netz geleitet.



Schematischer Aufbau: Der Protokollstapel des ZigBee-Protokolls baut auf den beiden unteren Layern (physical – PHY, Kanalzugriff – MAC) des IEEE-Standards 802.15.4 auf und beschreibt die Ebenen der Netzwerk- und der Anwendungsschicht. (Quelle: ZigBee Alliance)

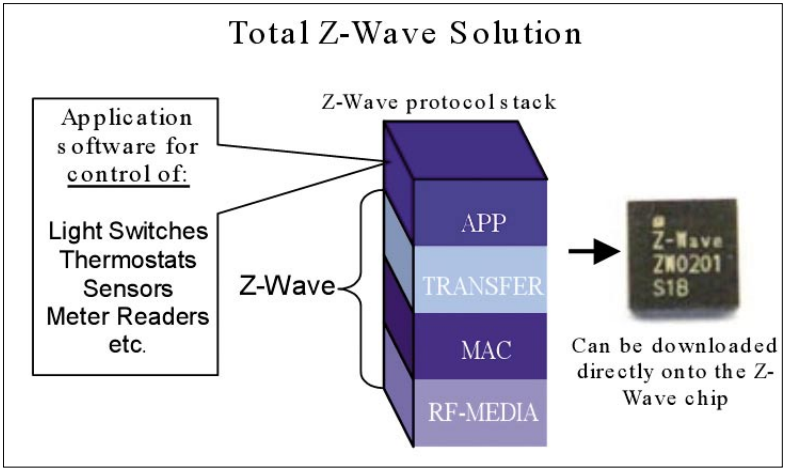
Die erste Version des ZigBee-Standards wurde nach vielen Diskussionen im Dezember 2004 verabschiedet. Sie deckt im Wesentlichen die Netzwerk- und die Anwendungsschicht ab. Hiermit erlaubt der ZigBee-Standard auf der Netzwerkebe-

ne die Verwendung von vermaschten und autonom gerouteten Netzwerken. Die Vereinheitlichung der Anwendungsebene erlaubt potenziell die Interoperabilität zwischen verschiedenen Herstellern. Zusätzlich wird eine sehr aufwendige, aber komplette Security-Funktionalität beschrieben.

Der ZigBee-Ansatz zeichnet sich durch einen sehr frühen Start und durch einen sehr breiten, herstellerübergreifenden Ansatz aus. Dies führt allerdings leider auch mancherorts zu deutlich verlangsamten Entwicklungs- und Entscheidungsprozessen, so dass schlankere, herstellerspezifische Alternativen am Markt gegenwärtig ebenfalls erfolgreich sind. Nichtsdestoweniger stehen für IEEE802.15.4- und ZigBee-konforme Entwicklungen zahlreiche Produkte großer Hard- und Softwarehersteller zur Verfügung.

1.2.7 Die Z-Wave-Technologie

Z-Wave ist eine zunächst proprietäre Technologie des US-dänischen Herstellers Zensys A/S (www.zen-sys.com), die zunehmend versucht, im Rahmen einer übergreifenden Z-Wave-Alliance (www.z-wavealliance.org) einen allgemeinen Status zu erlangen. Die Technologie basiert auf einem vorgegebenen IC und baut darauf ebenfalls mit den höheren Protokollschichten auf. Der zentrale Bestandteil der Z-Wave-Technologie ist ein Zwei-Wege-Kommunikationsprotokoll mit Mesh-Netzwerkfunktionalität. Die Bandbreite beträgt 9,6 kBit/s. Um trotz Signalstörungen (Noise, Distortion) eine sichere und zuverlässige Datenübertragung zu gewährleisten, besitzt Z-Wave ein 2-Wege-Acknowledgement und ein festes Frame-Format sowie einen Random-Back-Off-Algorithmus.

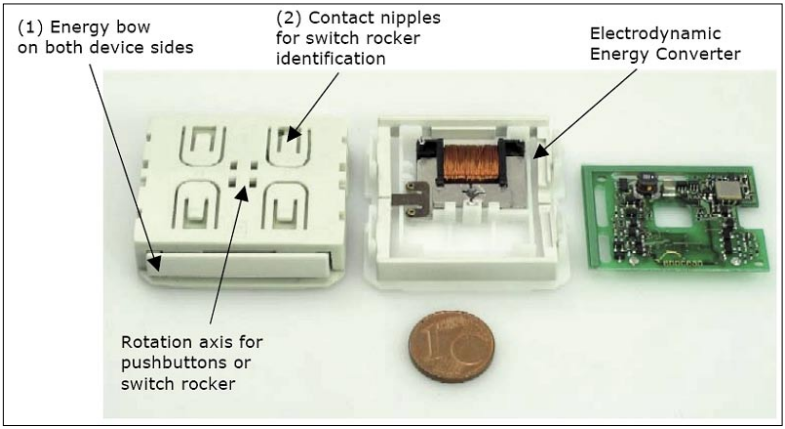


Basis: Der ASIC des Herstellers Zensys A/S ist die Grundlage für die Z-Wave-Funktechnologie. (Quelle: Z-Wave-Alliance)

Der Ansatz von Z-Wave ist insgesamt sehr schlank und effizient gehalten. Bislang haben verschiedene Hersteller für den Gebäudebereich diese proprietäre Technologie gewählt. Da bislang die Zertifizierung noch nicht sehr streng gehandhabt wurde, steht die Interoperabilität für die meisten Produkte noch aus.

1.2.8 EnOcean-Technologie im Detail

Einen komplett neuartigen Ansatz verwendet die deutsche Firma EnOcean (www.enocean.de), die als Spinoff aus der Siemens-Forschung hervorgegangen ist. Diese hat sich insbesondere dem Thema der Energieversorgung gewidmet, da es auch bei langen Batteriestandzeiten im Bereich von einigen Jahren als Problem erkannt wurde, wenn hunderte von batteriebetriebenen Funkknoten im Haus installiert sind. Deswegen haben die Ingenieure von EnOcean Energiewandler entwickelt, die die Wandlung von Energie aus der Umgebung erlauben. Die gegenwärtig wichtigste Komponente ist ein piezoelektrischer Druckwandler, der zum Beispiel in einem völlig autonomen Lichtschalter eingesetzt werden kann und Batterien komplett überflüssig macht.



Autonom: Die Energiewandler des deutschen Herstellers EnOcean erlauben die Entwicklung von völlig autonomen und energieautarken Funkknoten. (Quelle: EnOcean)

Diese Wandler werden mit einer speziellen Funktechnologie ausgestattet, die mit den kleinen Energieportionen haushälterisch umgeht. Mit diesem Ansatz hat sich das Unternehmen einen weltweiten Marktvorsprung herausgearbeitet und ist momentan der einzige Hersteller, der solche Produkte in Stückzahlen liefern kann.

Ein EnOcean-Funkmodul kann mit nur 50 µWs ein Signal über eine Entfernung von 300 m übertragen. Die Lösung des Geheimnisses liegt in der Signaldauer. Denn der gesamte Prozess wird ausgelöst, durchgeführt und abgeschlossen in ma-

ximal einer Millionstel Sekunde. Die Module arbeiten auf dem lizenzfreien 868,3-MHz-Band. Für die Datenmodulation verwendet der Hersteller die inkohärente Amplitudenmodulation (ASK). Diese digitale Amplitudenmodulation gewährleistet die Implementierung von energiesparenden Sendemodulen, da lediglich die einzelnen Bits übertragen werden. Darüber hinaus besitzt die EnOcean-Technologie eine geringe Kollisionswahrscheinlichkeit, da die Datenpakete in zufälligen Intervallen gesendet werden.

1.2.9 Fazit und Ausblick

Trotz der wesentlichen Fortschritte auf dem Gebiet der kleinen Funknetzwerke bleibt eine Reihe von technischen und organisatorischen Herausforderungen, die in der Zukunft gelöst werden müssen:

Die vorgestellten Technologien und ihre proprietären Geschwister sind allesamt nicht interoperabel. Vor allem bieten sie auch keine Schnittstellen für eine sinnvolle Zusammenarbeit, so dass eine Verschaltung nur auf der aufwendigen Gateway-Ebene (Layer 7) möglich ist. Zusätzlich verfügen die kleinen Funkknoten über sehr eingeschränkte Benutzerschnittstellen. Dies macht die Inbetriebnahme der Produkte manchmal sehr unhandlich.

Die Sicherheit von Funkübertragung ist eine wesentliche Voraussetzung für einen umfassenden Markterfolg. Leider wird dieses Thema bislang meist vernachlässigt. Selbst wenn kryptographische Verfahren von den Technologien vorgesehen sind, werden diese von den Produktherstellern nur selten genutzt.

Ein wichtiger Aspekt von Funknetzen entsteht auch durch übermäßige Nutzung dieser Technologien. Je mehr Funksysteme sich die lizenzfreien ISM-Bänder teilen müssen, desto mehr nimmt deren Auslastung zu. Die Koexistenzproblematik wird hierdurch immer kritischer.

Prof. Dr. Axel Sikora

tecCHANNEL-Links zum Thema	Webcode	Compact
Funknetzwerke für die Gebäudeautomation	448561	S.22
802.11: Standard für drahtlose Netze	401637	–
802.11 Standard für drahtlose Netze – Zukünftige Entwicklungen	429800	–
Grundlagen WiMAX – Anwendung, Architektur und Aufbau	433538	–
RFID – Die technischen Gundlagen	431196	–

1.3 Überwachungssysteme in Netzwerken

Um ein Unternehmensnetz gegen Angriffe sicher zu machen, braucht man ein fein abgestimmtes und gut funktionierendes Sicherheitsnetz. Eine der wichtigsten Komponenten ist dabei die Intrusion Detection beziehungsweise Intrusion Prevention (IDS/IPS). Intrusion-Detection- und Intrusion-Prevention-Systeme überwachen den Verkehr in einem Netzwerk und sollen Angreifer hindern. Sie schlagen bei Eindringlingen Alarm (IDS) oder ergreifen gleichzeitig Gegenmaßnahmen (IPS). Die Arbeitsweise von IDS und IPS sind annähernd gleich, bis auf den Unterschied, dass IPS Angreifer im besten Fall aussperren können. Die Systeme bestehen aus einzelnen Bausteinen, die unterschiedliche Aufgaben erfüllen.

In diesem Artikel wollen wir Ihnen die Arbeitsweisen beider Systeme näher bringen. Dabei werfen wir auch einen kurzen Blick auf Honeypots. Diese haben die Aufgabe, Angreifer abzulenken und Erkenntnisse über neue Attacken zu sammeln. Ausführlichen Hintergrundinformationen dazu finden Sie im Artikel „Der Einsatz von Honeypots“ (**Webcode 443579**).

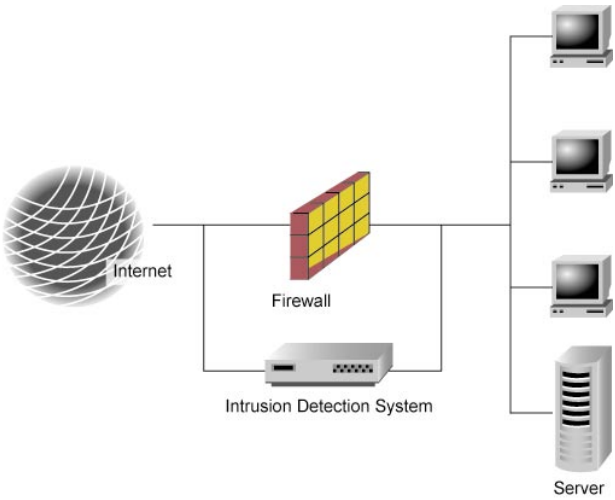
1.3.1 Funktionsweisen

Zu diesem Zweck muss zuerst der in Frage kommende Datenverkehr gesammelt werden. Je nachdem welche Intrusion-Detection-Technik zum Einsatz kommt, sammelt das System Daten aus dem Netzwerk, schaut also in die einzelnen Datenpakete hinein, oder aber es befasst sich mit Systemdateien wie zum Beispiel den Logfiles einzelner Server.

Anschließend analysiert das System diese Daten. Jedes Datenpaket kann theoretisch ein Angriff auf das Netzwerk sein, es wird aus diesem Grund auf verdächtige Spuren untersucht. IDS sucht bei der Analyse zum Beispiel nach bekannten Signaturen in „mitgelesenen“ Datenpaketen oder befasst sich näher mit Anmeldeversuchen, die nicht funktionierten. Sind die Daten untersucht, müssen die Ergebnisse weiterverarbeitet werden. Ist das System fündig, löst es zum Beispiel Alarm aus (IDS) oder leitet zusätzlich vordefinierte Gegenmaßnahmen ein, bevor der Angreifer Schaden anrichtet (IPS).

Lösungsansätze

Um mit IDS den Netzwerkverkehr zu beobachten, haben Administratoren verschiedene Möglichkeiten: Sie können das Firmennetz in Segmente aufteilen und in jedem Segment eine Überwachungs-Hardware positionieren, sie können aber auch eine Software auf allen zu schützenden Systemen installieren, wie zum Beispiel Web-, Mail- oder File-Servern.



Aufpasser: Netzwerkbasierte Intrusion-Detection-Systeme haben ein Auge auf den gesamten Netzwerk-Traffic

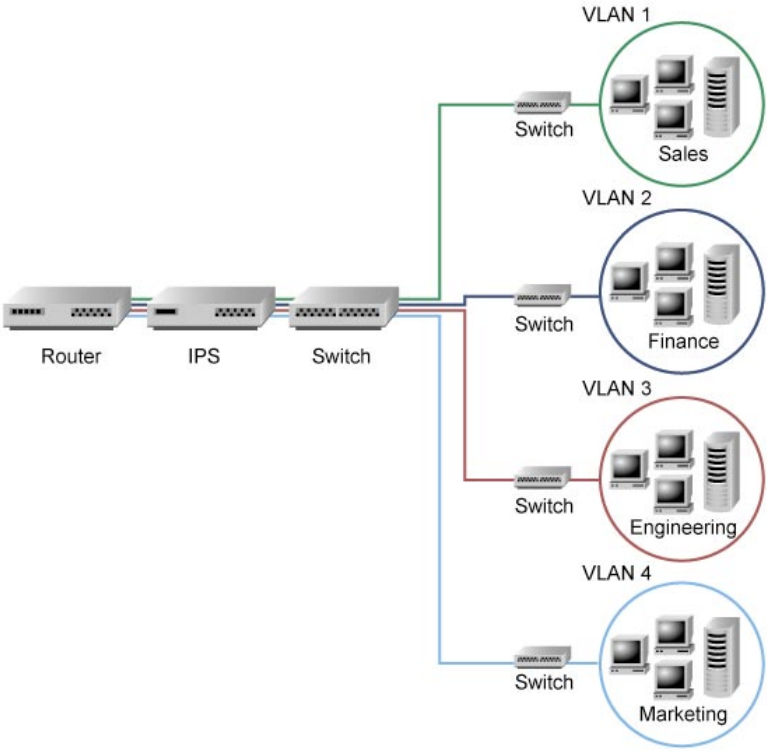
1.3.2 Network-based Intrusion Detection System (NIDS)

NIDS überwachen den gesamten Verkehr in einem Datennetz. Je nach der Größe des Netzwerks empfiehlt es sich, einzelne Segmente einzurichten. So werden die NIDS nicht überlastet. Sind NIDS im Netz platziert, beobachten und erfassen sie den gesamten Datenverkehr in ihrem Segment.

Durch die Analyse dieser Daten kann die IDS etwa anhand von Signaturen feststellen, ob es sich bei den gesammelten Daten um normalen Verkehr oder um einen Angriff handelt. Das System bedient sich einer vordefinierten „Roten Liste", in der gefährlicher Datenverkehr verzeichnet ist. Außerdem legt die Liste fest, wie mit diesen Daten zu verfahren ist. Da NIDS den ganzen Datenverkehr mitlesen sollen, müssen sie wohlüberlegt platziert sein. Überlastete NIDS können sich negativ auf das gesamte Netzwerk auswirken. Deswegen bestehen Network-based-Intrusion-Dectection-Systeme in der Regel aus mehreren logischen Bausteinen.

1.3.3 Aufbau eines NDIS

So genannte **Sensoren** sind die eigentlichen Schnüffler. Sie erfassen die Daten aus dem jeweiligen Netzsegment und senden sie zur Analyse an einen entsprechenden Baustein. Für die Verwaltung der Sensoren sorgt die **Managementstation**. Mit einer Managementstation lassen sich die Sensoren bedienen.

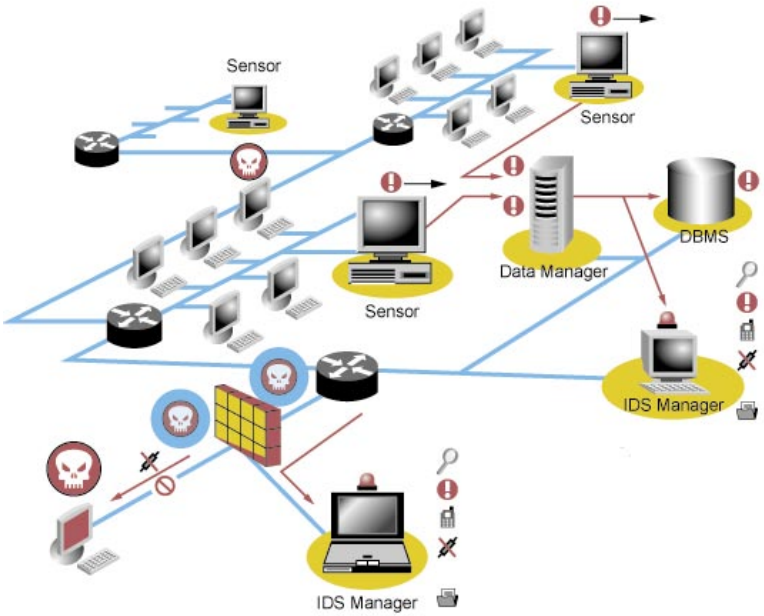


Skalierbar: Wenn es das Netzwerkaufkommen erfordert, können vor einzelne Switches noch zusätzliche Prüfsysteme geschalten werden.

Über eine Benutzeroberfläche können Administratoren auch die Ereignisinformationen anzeigen lassen, aus denen der Administrator ablesen kann, was gerade im Netzwerk passiert. Außerdem speichert die Managementkonsole Einstellungsparameter für die Sensoren.

Vor- und Nachteile eines NIDS

NDIS laufen auf eigenen Appliances, belasten also keine Endsysteme wie zum Beispiel Server. Zudem sind die Schnüffler für Angreifer schwer zu entdecken. Im so genannten Promiscuous Mode arbeiten die Systeme ohne eigene IP-Adresse und belauschen den Traffic nur passiv. Somit sind sie für Hacker schwierig aufzufinden. Netzwerkbasierte Systeme können zudem Angriffe erkennen, die sich nicht gegen ein bestimmtes Zielsystem richten.



Teamwork: IDS/IPS bestehen aus mehreren Komponenten wie Managementkonsole, Sensoren und Datenbanken.

Was spricht gegen ein NIDS?

Der größte Nachteil ist sicher, dass NIDS nicht das Verhalten des eigentlichen Angriffsziels sehen. Daher können sie so viel über die Attacke lernen und berichten, wie im Netzverkehr sichtbar war. Dazu kommt, dass NIDS in verschlüsselten Daten keine Ereignisse erkennen.

1.3.4 Host-based Intrusion Detection (HIDS)

HIDS laufen auf einzelnen Hosts, sammeln und analysieren alle Daten, die genau den Host betreffen. Sie interessieren sich nicht für den ganzen Netzwerkverkehr. Dadurch können HIDS, anders als NIDS, wesentlich genauere Aussagen über die Angriffsart machen. HIDS können den Angriff und die Folgen nachvollziehen, da sie selbst unmittelbar betroffen sind. HIDS beschäftigen sich nicht so sehr mit einzelnen Datenpaketen, sie überwachen mehr das System, auf dem sie laufen, und halten zum Beispiel Ausschau nach Trojanern. Zudem können sie auf Logfiles zugreifen, womit HIDS Einblick in Login-Versuche auf Betriebssysteme und Applikationen erhalten.

Auf der Heft-CD: Linux-Distributionen & Tools

Dieses tecCHANNEL-Compact enthält die begleitende Software zu den Artikeln auf einer CD-ROM. Sie finden auf unserem Datenträger:

Linux: Trinity Rescue Kit, SystemRescueCD und mehr

Mit dem bootfähigen Trinity Rescue Kit auf der CD erhalten Sie ein vielseitiges Werkzeug, wenn Ihr Windows oder Linux nicht mehr startet. Außerdem finden Sie die Distributionen grml, SystemRescueCD und QEMU-Puppy auf der CD.

Netzwerk-Tools: Werkzeugkiste für Administratoren

Wir stellen Ihnen in diesem Compact eine Sammlung hilfreicher Netzwerk-Utilities für Windows-Systeme vor, die dem Administrator das Leben erleichtern. Auf der CD finden Sie viele der nützlichen Helfer.

eBooks: VoIP-Spezial und Compact 3/2006 als PDF

Unser 72-Seiten-PDF zu den Grundlagen und Sicherheitsaspekten von VoIP und das tecCHANNEL Compact 3/2006 im Volltext runden die Heft-CD ab.

Bei technischen Problemen können Sie die Dokumentation, FAQ oder das Forum auf den Websites der jeweiligen Hersteller nutzen.

tecCHANNEL bietet keinen Support für Installation, Konfiguration oder Einsatz der Software auf der mitgelieferten CD-ROM.

Ihre CD fehlt, ist zerkratzt oder nicht lesbar?
Bitte Schreiben Sie an: tecCHANNEL Kundenservice, Postfach 81 05 80, 70522 Stuttgart,
Tel: (+49) 07 11/72 52-276, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15,
Fax: (+49) 07 11/72 52-377, E-Mail: shop@tecchannel.de

Vor- und Nachteile eines HIDS

HIDS laufen auf dem angegriffenen System selbst und können daher im Gegensatz zu NIDS die Reaktion des Hosts beobachten. Zudem müssen sie sich nicht mit dem ganzen Netzwerkverkehr befassen, nur mit dem, der die zu überwachende Plattform betrifft.

Schwächen der Host-basierten Intrusion Detection Systeme

HIDS sind vom Betriebssystem und den Applikationen auf dem jeweiligen Host abhängig. Für jede zu überwachende Hardware muss ein entsprechendes HIDS verfügbar sein. Zusätzlich brauchen die Überwachungsfunktionen Systemressourcen, der Betrieb belastet die zu überwachende Hardware. Im Gegensatz zu NIDS kann ein Angreifer eine Host-basierte Lösung einfacher erkennen.

1.3.5 Network Node-based Intrusion Detection (NNIDS)

NNIDS sind auch auf dem jeweiligen Zielsystem installiert. Der Vorteil ist, dass sie wie auch NIDS Datenpakete lesen und analysieren. Dabei beschränken sich allerdings auf Daten, die für das Zielsystem bestimmt sind, und auf solche, die von diesem gesendet werden. Zusätzlich beobachten NNIDS Ereignisse auf Betriebssystemebene (zum Beispiel fehlerhafte Anmeldeversuche).

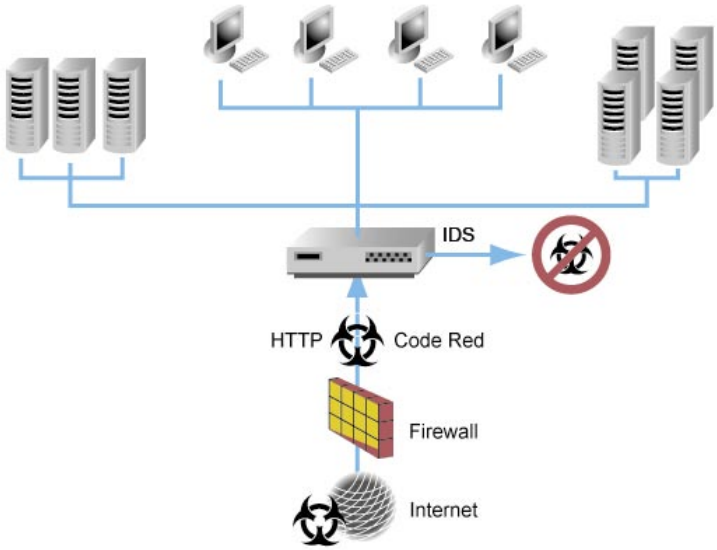
Vor- und Nachteile der NNIDS

Da anders als bei NIDS nicht jedes Datenpaket untersucht werden muss, ist die Leistung eines solchen Systems gegenüber der Netzwerklösung deutlich höher. Allerdings können NNIDS nicht im Promiscuous Mode laufen, sind somit für Angreifer leicht zu erkennen und werden unter Umständen selbst zum Angriffsziel. Wie HIDS benötigen sie außerdem Ressourcen auf dem installierten System.

1.3.6 Wie wird ein Angreifer erkannt?

Ziel der Intrusion-Detection-Systeme ist es, Angriffe zu erkennen und Alarm zu schlagen. Um einen Angriff zu erkennen, müssen die geschnüffelten Daten analysiert werden. Es gibt zwei verschiedene Arten, Angriffe zu entdecken: Missbrauchs- und Anomalieerkennung.

Eine „beste Erkennungsmethode“ gibt es nicht, Sinn macht erst die Kombination der beiden Methoden. NIDS und NNIDS forschen meist nach Missbrauch und verbinden hier die Protokollanalyse mit Pattern Matching und Anomalieerkennung. Host-basierende Intrusion Detection Systeme setzen vor allem auf Anomalieerkennung, sind aber in ihrer Leistung eingeschränkt, da immer definiert sein muss, was normal ist und was nicht.



Keine Chance: Unter Umständen lässt die Firewall einen Angreifer durch, weil genau dieser Datenstrom freigegeben ist, das IDS liest aber in jedem einzelnen Paket und kann so einen Angriff dennoch abwehren.

1.3.7 Erkennen von Missbrauch

Die Missbrauchserkennung beruht auf bekannten Angriffsmustern. Über ein so genanntes **Pattern Matching** (Bitmuster/Abgleich) untersucht das IDS den Datenstrom auf bekannte (Angriffs-)Bitmuster und vergleicht die gesammelten Daten laufend mit einer Datenbank.

Dadurch ist der Rechenaufwand beim Pattern Matching groß. Wenn das Netzwerk ohnehin stark ausgelastet ist, ist ein solcher Abgleich aller Datenpakete mit den Datenbanken kaum möglich. Es ist also ratsam, sich bereits vor der Installation eines IDS genau zu überlegen, wie sich das Netz am besten segmentieren lässt. So lassen sich Flaschenhälse durch ein NIDS bereits im Vorfeld verhindern.

Alternative: Protokollanalyse

Eine andere Möglichkeit, Angreifern auf die Schliche zu kommen, ist die **Protokollanalyse**. Ein sogenanntes „Normalverhalten“ im Netzwerk ist in den Protokollspezifikationen hinterlegt. IDS untersucht die Daten in den Datenpaketen mit Hilfe vorliegender Protokollinformationen und entscheidet, ob der Datenverkehr die Protokollspezifikationen erfüllt. Im Vergleich zum Pattern Matching ist der Rechenaufwand deutlich geringer.

1.3.8 Voraussetzungen

Unabhängig von beiden Methoden stellt die Missbrauchserkennung allerdings einige Anforderungen: Ein Angriff lässt sich nur erkennen, wenn er schon als Angriff bekannt und in der Signaturdatenbank hinterlegt ist. Des Weiteren muss diese bekannte Angriffssignatur dem IDS zugänglich gemacht werden, damit dieses die eingehenden Datenpakete vergleichen kann. Eine Signaturdatenbank ist daher immer ein zentraler Bestandteil des IDS.

Um eingehende Daten als gefährlich zu erkennen, müssen sie analysiert werden. Datenpakete werden allerdings mitunter in kleine Segmente zerlegt und ohne eine bestimmte Reihenfolge über das Netzwerk versendet. Sie schlagen also unter Umständen durcheinander und nicht hintereinander auf dem IDS auf. Das Intrusion Detection System muss die Datenpakete erst wieder in die richtige Reihenfolge bringen und die einzelnen Teile zusammensetzen, um die Nutzdaten vollständig überprüfen und abgleichen zu können.

1.3.9 Suche nach Anomalien

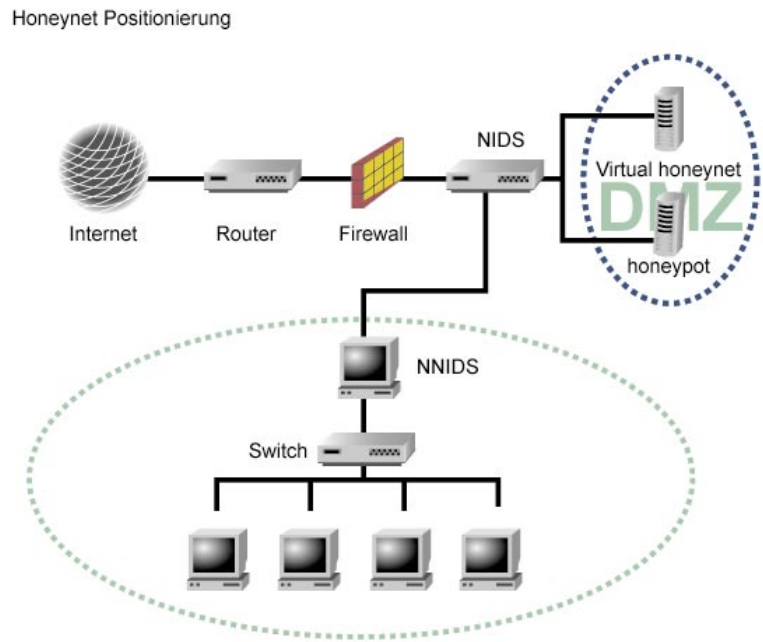
Eine weitere Möglichkeit, das Netzwerk nach Störenfrieden abzusuchen, ist die Anomalieerkennung. Dabei versucht das System Abweichungen vom Normalbetrieb zu erkennen. Die Schnüffler im Netz oder auf den Hosts halten Ausschau nach atypischen Verhaltensweisen des zu überwachenden Systemabschnitts. Um das System auf solche Ungereimtheiten zu untersuchen, muss zunächst einmal definiert sein, was „Normalzustand“ bedeutet. Was normales Verhalten ist und was nicht, lässt sich über logische oder statistische Ansätze festlegen.

Bei einer Anomalieerkennung mit Hilfe statistischer Daten geht das System davon aus, dass das Netzwerk im Falle eines Angriffs stark von den statistischen Kennzahlen des Netzes abweicht (zum Beispiel Datenaufkommen und Art der Pakete, Zahl der Anmeldeversuche). Das Normalverhalten eines Netzes wird in einer „roten Liste“ hinterlegt. Diese Liste kann verschiedene Angaben enthalten: Datenverkehr entsprechend der Tageszeit, CPU-Auslastungen, Zugriffsdauer, Nutzungshäufigkeit. Diese Mittelwerte samt Toleranzgrenzen sind auf dem System hinterlegt. Anomalie auf statistischer Basis kann nur als ergänzendes Erkennungsverfahren gelten, da Angriffe sehr wohl in einer normalen Umgebung stattfinden können und dann nicht als abnormal erkannt werden. Die Statistik hinterfragt allerdings nicht die zeitliche Abfolge der einzelnen Ereignisse. Unregelmäßigkeiten in dieser Abfolge könnten jedoch auch auf einen Angriff hinweisen.

Deshalb berücksichtigt eine programmierbare Logik auch die zeitliche Abfolge von Ereignissen. Auch hier ist das Normalverhalten in Regeln zusammengefasst. Wenn Angriffe also eine bestimmte Ereignisfolge bedingen, die nicht als Normalzustand des Netzes definiert sind, erkennen IDS diese Ereignisse als Anomalie.

1.3.10 Honeypots – Honigtöpfe für gierige Datendiebe

Honeypots stellen eine gute Möglichkeit dar, um die Anomalieerkennung zu verfeinern. Dabei handelt es sich um dezidierte Systeme im Netzwerk, die keine kritische Funktion erfüllen. Sie sind Fallen für Angreifer, täuschen sicherheitskritische und produktive Systeme vor.



Verlockend: Honeypots und Honeynets sammeln Daten über Angreifer und deren Methoden.

Ein Honigtopf hat ein einfaches Normalverhalten: Es gibt nur wenige, vordefinierte Zugriffe auf das System, somit ist jeder Zugriff außer den vordefinierten anormal. Auf diese Art lassen sich Angriffe prima aufzeichnen und nachuntersuchen. Eine Prüfung der verschiedenen Angriffe deckt Fehlverhalten des eigenen Systems auf, die Schwachstellen können besser nachvollzogen und gegebenenfalls beseitigt werden.

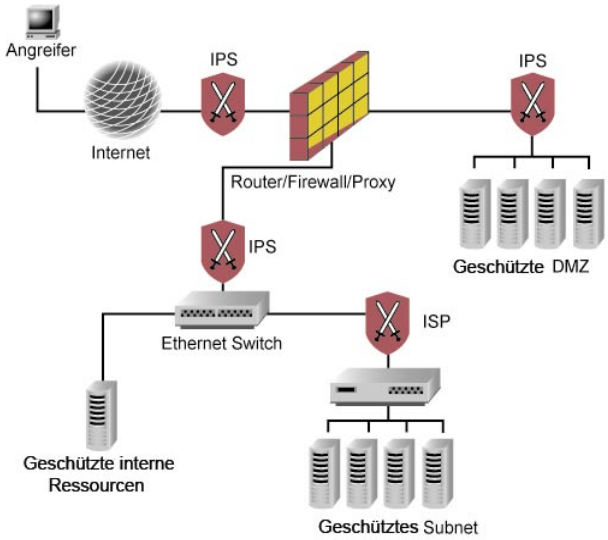
Mehr rund um das Thema Honeypots haben wir für Sie in unserem Artikel „Der Einsatz von Honeypots“ (**Webcode 443579**) zusammengestellt. Darin erfahren Sie Wissenswertes über die beiden Honeypot-Lösungen Tiny Honeypot und honeyd. Zudem erklären wir Ihnen die Installation und Verwendung.

1.3.11 Angriffsabwehr mit Intrusion-Prevention-Systemen (IPS)

Intrusion-Prevention-Systeme (IPS) sind eine Weiterentwicklung des IDS. Während IDS Angriffe nur erkennen können und protokollieren, sind IPS in der Lage, Angriffe abzuwehren. Hierfür gibt es zwei Arten von Abwehr: das IPS sitzt irgendwo im Übertragungsweg und sperrt beziehungsweise verwirft Datenpakete, die als Angriff erkannt wurden.

Die andere Möglichkeit ist, dass die IPS die Regeln für die Paketfilter beziehungsweise Application Level Gateway so anpassen, dass schädlicher Verkehr hierüber ausgefiltert wird. Wie bei IDS gibt es Systeme, die im Netz hängen, und Einheiten, die auf Hosts laufen. Angriffe erkennen IPS genau wie IDS über die Signaturen in den Paketen oder über Anomalien im Betrieb und im Datenstrom.

Das Wichtigste an einem IPS ist die Reaktionszeit. Um Angreifer auszusperren, muss das IPS alle Daten kontrollieren und bei Bedarf Gegenmaßnahmen einleiten, zum Beispiel temporäre Filter in der Firewall oder Unerreichbarkeitsmeldungen über ICMP an den angreifenden Rechner. Bis das alles abgeschlossen ist, kann der Angreifer schon durchgebrochen sein. Das IPS hat nur eine Chance, wenn es direkt im Übertragungsweg sitzt. So kann es Pakete sofort löschen anstatt sie weiterzuleiten. Zusätzlich kann es anschließend alle anderen ankommenden Daten der gleichen Verbindung löschen.



Aktive Gegenwehr: Intrusion-Prevention-Systeme kontern erkannte Attacken nach vorher festgelegten Parametern.

1.3.12 Verteidigungsszenarien mit IPS

IPS können auf zwei Arten arbeiten: Bei der so genannten **Fail-open-Technik** werden bei einem festgestellten Angriff sofort Gegenmaßnahmen eingeleitet. Im Anschluss wird der nachfolgende Verkehr nicht überwacht, der Betrieb läuft ganz normal weiter. Anders bei der **Fail-close-Strategie**: Bei einem Angriff wird der Datenstrom sofort unterbrochen, ähnlich einer Firewall.

Für eines der beiden Konzepte muss sich der Administrator entscheiden, bei Fail open kann es sein, dass nach erkanntem Angriff zwar der Bösewicht beseitigt wird, nachfolgender bösartiger Verkehr kann das IPS aber ungehindert passieren. Bei Fail close dagegen ist das IPS schnell selber das Angriffsziel, welches sich durch DoS-Attacken lahmlegen ließe.

Eine andere Gefahr sind falsche Alarme (False Positives). Während ein IDS nur falsch alarmiert, schließt ein IPS unter Umständen bei falschem Alarm das ganze Netz, beziehungsweise echter bösartiger Verkehr dringt ins Netzwerk ein, weil das IPS gerade fälschlicherweise mit einem Angreifer beschäftigt ist. IPS sollten deshalb so konfiguriert sein, dass sie nur dann eingreifen, wenn es sich bei den beobachteten Datenpaketen ganz sicher um einen Angreifer handelt, ähnlich der Toleranzen eines IDS.

1.3.13 Fazit

IDS und IPS sind allerdings keine Garanten für ein abgeschottetes Netzwerk. Dennoch sind sie wichtige Teilbereiche in einem umfassenden Sicherheitskonzept. IDS und IPS bedürfen einer Administration und der Wartung, um zu funktionieren. Zudem müssen sie in bestehende und funktionierende IT-Infrastrukturen integriert sein. Ein sauberes Zusammenspiel zwischen den Systemen entscheidet dann langfristig über den Nutzen solcher Sicherheitswerkzeuge.

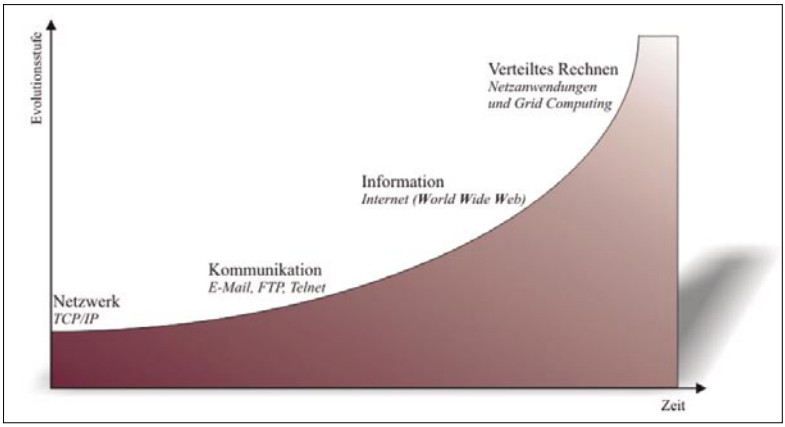
Dennoch machen beide Systeme Sinn. Gerade wenn Ihre Firma im Internet mit mehr als nur einer Homepage präsent ist, sind die Online-Funktionen vitale Teilbereiche. Eine Störung kann für empfindliche Umsatzeinbußen sorgen. Durch die Signaturprüfungen lassen sich vor allem bekannte Angriffe effektiv abwehren. So schützen Sie sich effektiv gegen Script-Kiddies und andere „Zufallsattacken“.

Andreas Wurm

tecCHANNEL-Links zum Thema	Webcode	Compact
Überwachungssysteme in Netzwerken	454641	S.31
Praxis: Einsatz von Honeypots	443579	–
Grundlagen: Das müssen Sie über Honeypots wissen	431426	–

1.4 Networked Computing: Grundlagen und Anwendungen

Dass das Ganze mehr ist als die Summe seiner Teile bewahrheitet sich auch bei Rechnernetzen. Der intelligente Zusammenschluss von Rechnern bringt neue Technologien hervor, die weit über das hinausgehen, was gewöhnliche Client-Server-Strukturen in Unternehmen leisten.



Nächster Schritt: Grids & Co. sind die nächste Evolutionsstufe in der IT. (Quelle: Norbert Fuhr)

Cluster-, Grid-, Peer-to-Peer- und Distributed Computing sind die wichtigsten dieser Rechnerverbünde. Sie spielen in Wissenschaft und Wirtschaft zum Teil bereits heute, zum Teil in den nächsten Jahren, eine herausragende Rolle. Viele Fachleute interpretieren diesen Komplex der Vernetzung und des verteilten Rechnens auf Verbundbasis als nächsten Evolutionsschritt in der IT, der Internet und WWW hinter sich lässt.

1.4.1 Cluster: Einsatzbereiche

In vielen Unternehmen schon heute verbreitet sind Cluster. Sie werden dort eingesetzt für Lastverteilungs- oder Hochverfügbarkeitslösungen – etwa im Bereich von Datenbank- und Webservern. Über die Kopplung von Rechnern kann gewährleistet werden, dass Rechenanforderungen gleichmäßig verteilt werden oder kritische Systeme nach dem Ausfall eines Servers problemlos weiter arbeiten.

Die Idee des Grid Computing ist hingegen im kommerziellen Bereich noch weitgehend neu. Anders als bei Clustern zapft man bei Grids die Ressourcen externer Rechner oder auch ganzer Cluster an, virtualisiert und integriert sie. Eine natürli-

che Tendenz für Grids ist dabei die Ausdehnung auf immer größere Benutzergruppen und Communities. Eng verwandt mit Grids und oft zusammen in einen Topf geworfen wird die Technik des Distributed Computing. Im Vordergrund steht hier das Lösen einer rechenintensiven Aufgabe, die auf mehrere, meist weltweit verstreute Rechner verteilt wird.

P2P-Systeme dürften wiederum für die meisten alte Bekannte sein. Sie haben sich in der Praxis vor allem in Form der umstrittenen Tauschbörsen bewährt, sind aber auch für andere Einsatzgebiete geeignet. Wie sich die einzelnen Rechnerverbünde genau definieren, worin sie sich unterscheiden und welche Anwendungen es gibt stellen wir in diesem Beitrag vor.

1.4.2 Cluster: Das Grundprinzip

Bei einem Cluster werden mehrere unabhängige Computer über Software und Netzwerk zu einem Verbund von Rechnern vereinigt. Es besteht aus mindestens zwei Computern – im Fachjargon „Knoten" -, die über eine Verbindungstechnik wie Ethernet miteinander gekoppelt sind. Die Knoten sind in der Regel normale Standard-PCs, zum Teil auch Workstations, Server oder gar Supercomputer. Nach außen hin verhalten sich die Knoten in einem Cluster wie ein virtueller Prozessor. Das Ganze wirkt wie ein einziger Rechner, der Aufträge entgegen nimmt, auf die einzelnen Knoten verteilt und bearbeitet.

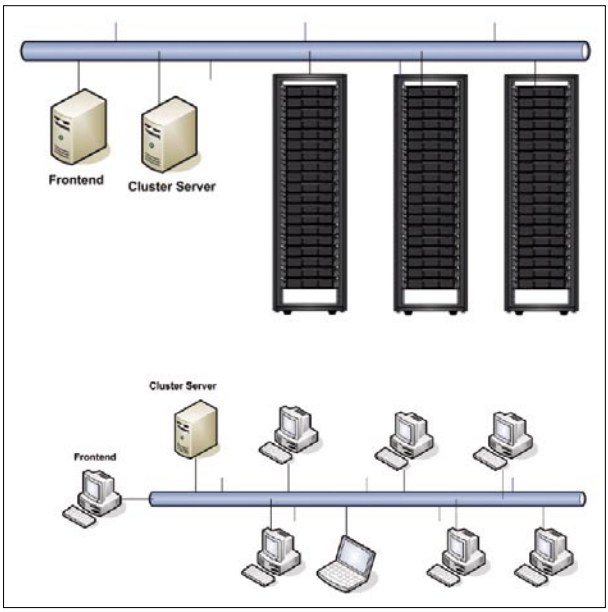
Im Vergleich zu einem leistungsstarken, teuren Superrechner hat ein Cluster vor allem zwei Vorteile: Es setzt sich normalerweise aus billigen Low-Cost Komponenten zusammen und ist skalierbar. Das Cluster kann jederzeit vergrößert werden, indem einfach neue Rechner dem System zur Verfügung gestellt werden.

Ist die Hard- und Software auf allen Knoten identisch, handelt es sich um ein homogenes, andernfalls um ein heterogenes Cluster. Von einem Cluster im engeren Sinn spricht man erst dann, wenn die Knoten exklusiv zum Verbund gehören und einen gemeinsamen Datenbestand verarbeiten.

1.4.3 Cluster: Aufbau

Für die Verbindung kommt bei kleineren Clustern aus Kostengründen Fast- oder Gigabit-Ethernet zum Einsatz. Größere Cluster werden gerne mit Hochgeschwindigkeitsnetzen wie SCI (Scalable Coherent Interface), Infiniband oder Quadrics betrieben. Letztere bieten nicht nur hohe Übertragungsgeschwindigkeiten, sondern auch niedrige Latenzzeiten. Dafür sind sie auch entsprechend teuer.

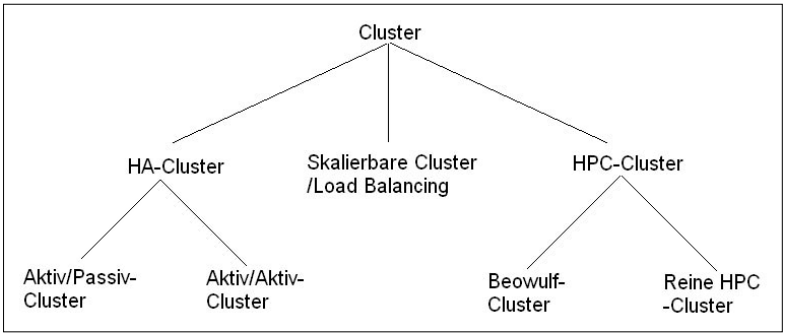
Zu bedenken ist auch, dass mit der Größe eines Clusters die Kommunikationskosten steigen. Je mehr Knoten ein Cluster umfasst, um so höher ist der Anteil an der Gesamtrechenleistung, den das Cluster für die Administration aufwenden muss.



Standard: Der typische Aufbau eines Clusters mit Clients, Cluster-Server und einem Frontend zur Verwaltung.

1.4.4 Hochverfügbarkeits-Cluster

In der Praxis werden Cluster-Systeme vor allem für drei Zielanwendungen eingesetzt. Hohe Ausfallsicherheit, hohe Rechenleistung und hoher Datendurchsatz. Hohe Ausfallsicherheit wird mit Hochverfügbarkeits- oder HA-Clustern (High Availibility Cluster) erreicht.



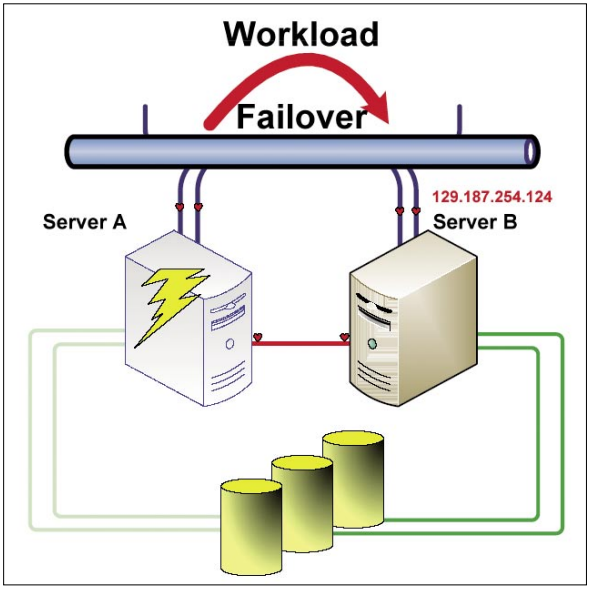
Im Focus: Die drei grundlegenden Cluster-Typen im Überblick.

Dazu koppelt man beispielsweise einen kritischen Datenbank-Server mit einem zweiten Rechner. Tritt auf dem Datenbank-Server ein Fehler auf, werden die auf diesem Rechner laufenden Dienste auf den anderen Knoten migriert. Das Zweitsystem übernimmt im Fehlerfall die Aufgaben des Primärsystems.

Bei HA-Clustern unterscheidet man zwischen Aktiv/Passiv- und Aktiv/Aktiv-Clustern. Sind beide Knoten aktiv (Aktiv/Aktiv) ist eine Lastverteilung zwischen den Knoten möglich. Bei Ausfall des einen Knotens übernimmt der andere dessen Arbeit ganz. Bei einem Aktiv/Passiv-Cluster arbeitet dagegen immer nur ein Server – das Primärsystem. Der zweite, wartende Server ist das Standby-System und muss bei Ausfall des Primärsystems aktiviert werden.

1.4.5 Einsatzgebiet und Verwaltung der HA-Cluster

In der Praxis spielen HA-Cluster bei unternehmenskritischen Anwendungen wie Datenbank, Webserver oder E-Mail eine große Rolle. Auch in hoch kritischen Umgebungen, in denen maximale Ausfallzeiten von nur wenigen Minuten im Jahr erlaubt sind, leisten HA-Cluster gute Dienste.



Notsituation: Verstummt in einem HA-Cluster der Heartbeat werden die Dienste des Primärsystems (links) vom Standby-System (rechts) übernommen. (Quelle: LRZ München)

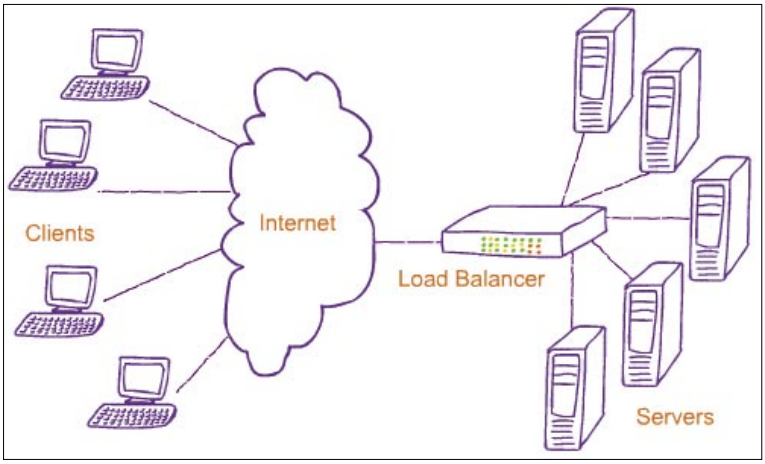
Wenn kritische Computersysteme für Katastrophenszenarien abgesichert werden, werden die Cluster-Knoten oft mehrere Kilometer getrennt in verschiedenen Rechenzentren platziert. Tritt der „worst case“ ein, kann der Knoten im nicht betrof-

fenen Rechenzentrum dann die gesamte Last übernehmen. Diese Art räumlich weit verteilter Cluster nennt man auch „stretched Cluster“. Für die Verwaltung von HA-Clustern stehen Cluster Manager zur Verfügung, die Vorgänge wie den Failover vom Primärsystem zum Standby-System im Fehlerfall automatisieren. Um den Ausfall eines Rechners im Cluster zu erkennen wird meist der so genannte Cluster Heartbeat in Verbindung mit einer Voting Disk verwendet – ein Signal, das über eine Netzwerkverbindung zwischen den Clusterknoten ausgetauscht wird. Verstummt der Heartbeat eines Rechners kann man einen Ausfall annehmen und ein Failover einleiten. Damit wird die Übernahme der Dienste vom Primärsystem – wie Datenbank-, Web- oder Application Server – auf das Standby-System initiiert.

Eine solide Open-Source-Basis ist das Linux-High-Availability-Projekt, kurz Linux-HA (http://linux-ha.org/). Dessen Ziel ist es, Linux-Systeme zur Hochverfügbarkeit aufzurüsten. Heartbeat, das kürzlich in der Version 2.0 frei gegeben wurde, ist dabei die Kernkomponente des Projektes. Ein relativ weit verbreitetes kommerzielles System ist Oracle RAC (Oracle Real Application Cluster, www.oracle.com/technology/products/database/clustering/index.html), eine zusätzliche Option des Datenbankmanagementsystems von Oracle.

1.4.6 Load Balancing und High Performance Cluster

Die zweite Anwendung von Clustern ist das Load-Balancing. Load-Balancing-Cluster verteilen die Rechnerlasten auf mehrere Maschinen. Statt durch Aufrüstung einzelner Computer wird der Performancebedarf hier durch das Hinzufügen zusätzlicher Computer erfüllt. Die Lastverteilung erfolgt in der Regel über eine redundant ausgelegte, zentrale Instanz, den Load Balancer.



Alle für einen: Load Balancer verteilen die Rechnerlasten auf mehrere Maschinen.

Mögliche Einsatzgebiete sind Umgebungen mit hohen oder wechselnden Anforderungen an die Computerperformance. Typisches Beispiel sind Shop-Systeme, die zu bestimmten Zeiten wie vor Weihnachten höher belastet sind.

Die dritte Cluster-Applikation ist die Verteilung von Rechenaufgaben. High Performance Cluster (HPC) dienen zur Abarbeitung von Rechenaufgaben, die auf mehrere Knoten distributiert werden. Dazu werden die Aufgaben in „Portionen" aufgeteilt und parallel auf mehreren Knoten ausgeführt. HP-Cluster finden sich oft im wissenschaftlichen Bereich.

1.4.7 Beowulf und Wolfpack

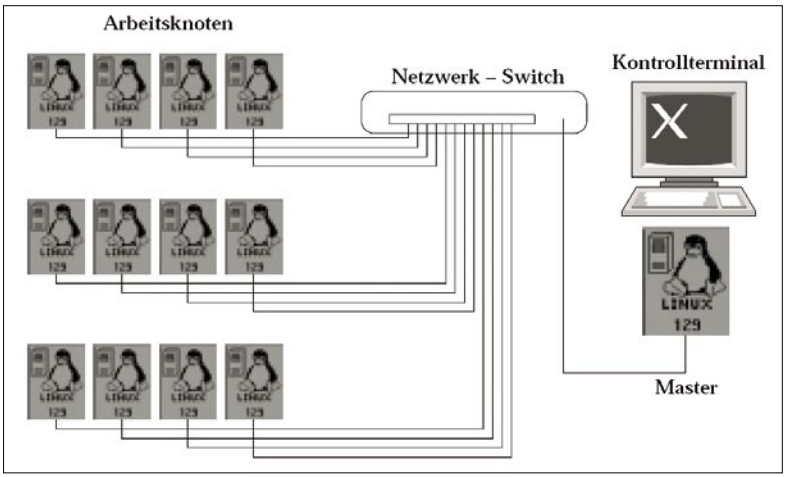
Leider lässt sich nicht jedes Rechenproblem durch ein HP-Cluster schneller lösen. Um Nutzen aus dem Cluster zu ziehen, muss sich das Problem auf mehrere Computer verteilen lassen. Das ist nicht immer möglich, beispielsweise dann nicht, wenn man Berechnungen anstellt, deren Teilergebnisse sich auf Teilergebnisse vorheriger Rechnungen beziehen. Oft kommt es auch vor, dass die Knoten untereinander viele Daten austauschen müssen oder dass sie ständig auf einen gemeinsamen Datenbestand wie etwa eine Datenbank zugreifen müssen. Dienen die Knoten in einem Cluster ausschließlich zum Berechnen und bestehen sie aus handelsüblichen PCs, die unter Linux laufen, spricht man von einem Beowulf-Cluster. Läuft Windows, ist es ein Wolfpack-Cluster.

Besonders beliebt sind Beowulf-Cluster (www.beowulf.org). Ihnen gemeinsam ist, dass die Knoten aus Standardkomponenten zusammengebaut werden, auf denen ein freies Betriebssystem arbeitet. Von der Einordnung her liegen Beowulf-Cluster zwischen reinen High Performance Clustern und COWs, Cluster of Workstations. Anders als bei einem COW, einem reinen Verbund aus Workstations, sind im Beowulf-Cluster alle Knoten exklusiv dem Cluster unterstellt.

1.4.8 Beowulf Cluster

Beowulf-Cluster stammen ursprünglich von den beiden NASA-Wissenschaftlern Thomas Sterling und Donald Becker, die 1994 einen Parallelrechner aus handelsüblichen Komponenten „von der Stange" bauen wollten. Ihr Ziel war es, einen billigen, aber effizienten und leistungsfähigen Supercomputer zu konstruieren, der es ihnen ermöglicht, große Datenmengen auszuwerten. Beowulf-Cluster verfügen typischerweise über keine Eingabegeräte oder Periphere, nur ein dedizierter Master-Rechner kommuniziert mit dem Cluster.

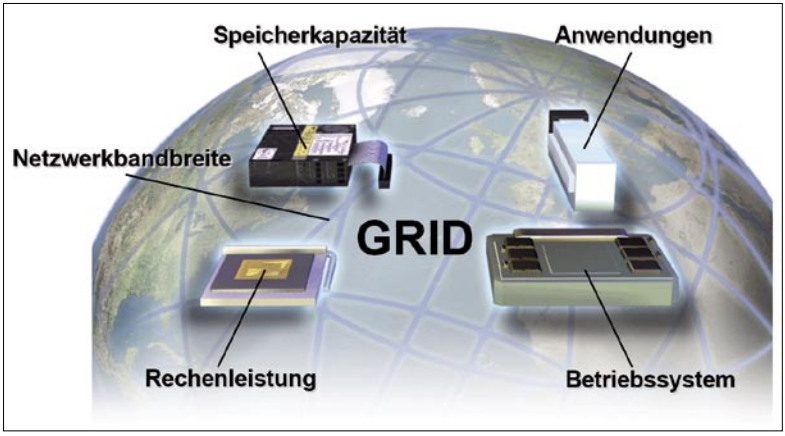
Das erste lauffähige System bestand aus 16 Knoten mit Intel 486-DX4-Prozessoren, das über ein 10 Mbit/s schnelles Ethernet verbunden waren. Für die Kommunikation wurde ein Nachrichtenaustauschsystem installiert. Inzwischen haben es einige Beowulf-Cluster in die Top500-Liste der schnellsten Supercomputer der Welt (www.top500.org) geschafft.



Im Detail: Der prinzipielle Aufbau eines typischen Beowulf Clusters. (Quelle: TU Graz)

1.4.9 Grid Computing

Einen Schritt weiter als Cluster Computing geht Grid Computing. Grids – abgeleitet von Electrical Power Grid, dem Stromnetz – sind ebenfalls komplexe IT-Rechner-Verbünde, allerdings mit sehr hohem Abstraktionsgrad.



Grids anschaulich: Die Verbundtechnologie Grid Computing virtualisiert weltweit verteilte in sich autonome IT-Ressourcen. (Quelle: Fraunhofer Institut)

Im Unterschied zum Cluster nehmen Grids verteilte Ressourcen externer Rechner, die verschiedenen Organisationen angehören können, in Anspruch. Die NASA beispielsweise nutzt ein Grid, wenn ein Flugzeug Probleme meldet. In diesem Fall durchkämmt eine Grid-Software quer über die USA verteilte Datenbanken, um Informationen über die Maschine zu finden.

Der Schlüsselterm beim Grid-Computing ist der Begriff der „Ressource“. Eine Ressource ist ein IT-Element, das in ein Grid eingebunden wird – etwa spezielle Hardware, Prozessorleistung, Datenbanken, Dateien oder Software. Im Grid werden diese Ressourcen in einer virtuellen Organisation integriert und über das Internet zugänglich gemacht. Über eine Schnittstelle lässt sich feststellen, welche Ressourcen vorhanden oder gerade frei sind, um diese dann gezielt anzusprechen. Dabei ist die geographische Position der Ressource nicht mehr von Interesse.

1.4.10 Unterschiede: Cluster und Grid

Die Unterschiede zwischen Grid und Cluster müssten damit bereits deutlich sein. Ein Cluster stellt nur reine Rechnerleistung zur Verfügung, und das auf lokal begrenztem Gebiet. Ein Grid hingegen stellt über die eigentliche Rechnerleistung hinaus auch Daten, Applikationen etc bereit – und das nicht nur lokal, sondern weltweit. Die folgende Tabelle listet die Unterschiede im Detail auf.

Unterschied Cluster ⇔ Grid

Cluster	Grid
• Verbund von mehreren Rechnern	• Verbund von mehreren Ressourcen
• Kommunikation über LAN	• Kommunikation über WAN
• gemeinsamer lokaler Standort	• verteilte Standorte
• zentraler Admin	• Jede Maschine eigener Admin
• Existenz des Clusters wegen Berechnungen	• Existenz des Grids aus verschiedenen Gründen
• Cluster ist Hauptarbeit der Rechner	• Grid ist Nebenarbeit der Ressourcen

Im Überblick: Cluster und Grid im Vergleich. (Quelle: Marco Heinrich)

Formal ist ein Grid durch drei typische Merkmale gekennzeichnet.

- Die Kommunikation erfolgt in der Regel über das Internet,
- es koordiniert dezentrale Ressourcen und
- es verwendet offene, standardisierte Protokolle und Schnittstellen.

Einen Software-Architekturstandard für Grid-Systeme beschreibt derzeit die Open Grid Service Architecture (OGSA, www.globus.org/ogsa). Das von der Globus Alliance (www.globus.org) entwickelte Globus Toolkit ist derzeit die einzig verfügbare Implementierung von OGSA, sie gilt als De-facto-Standard. Nähere und zusätzliche Details zu Grid-Standards und -Software erfahren Sie in einem eigenen im Beitrag „Grid-Technologie“ (**Webcode 435980**).

1.4.11 Arten von Grids

Es existieren mehrere Varianten von Grids, die wir im Folgenden näher erläutern:

Data Grids

Je nach Art der vernetzten Objekte und nach Anwendungsszenarien lassen sich mehrere Typen von Grids unterscheiden. Die dominierenden Grids sind Computational Grids. Bei diesen Grids geht es vor allem um Rechenleistung – die Ressourcen jedes einzelnen Rechners werden zusammengefasst, um die Gesamtrechenleistung zu erhöhen. Eine typische Anwendung ist das On-Demand-Computing.

Bei Data Grids steht statt Rechenleistung der Zugriff auf verteilte Datenbestände im Vordergrund. Das oben erwähnte NASA-Beispiel wäre ein Data Grid. Es nutzt geographisch verteilte Datenpools, daneben können auch Data Warehouses oder digitale Bibliotheken eingebunden werden. Zahlreicher als reine Data Grids sind Grids, bei denen geographisch verteilte Daten rechenintensiv bearbeitet werden. Dabei werden die Daten mit zusätzlicher verteilter Rechenkapazität über WWW-Schnittstellen gleich verarbeitet. Computational Grids und Data Grids können unter Resource Grids subsumiert werden. Die allgemeinen Eigenschaften dieser Grids sind, dass sie Betriebsmittel für verteilte Anwendungen bereitstellen.

Service Grids

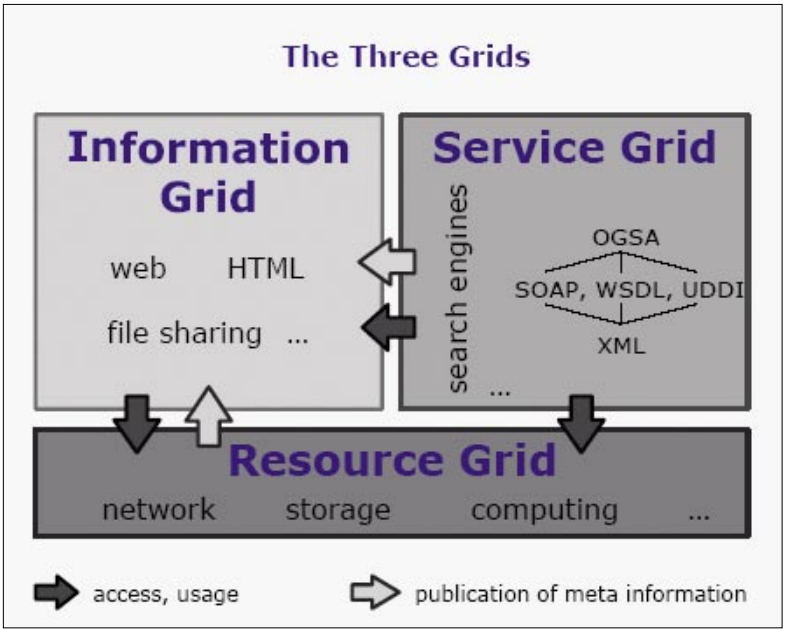
Der zweite, wichtige Typ von Grids neben Resource Grids sind Service Grids. Ein Service Grid ist abstrakter als ein Resource Grid – es bildet die Betriebsmittel der Resource Grids auf eine höhere Ebene ab. In einem Service Grid treten damit die Ressourcen selbst nicht mehr in Erscheinung – auch nicht in virtualisierter Form. Gegenüber den Benutzern werden nur noch „Dienste“ angeboten, die bei der Auftragsbearbeitung auf die geeigneten Ressourcen zugreifen. Für ein Service Grid sind Standards wie OGSA, XML, SOAP, UDDI, WSDL und WSRF relevant.

Service Grids werden häufig mit einem Rollenmodell assoziiert, in dem verschiedene Resource-Provider ihre Ressourcen als „Utilities“ in das System einbringen.

Der Grid-Service-Provider übernimmt den Nutzungsservice, definiert das Dienste-Spektrum und rechnet sowohl gegenüber den Resource-Providern als auch gegenüber den Benutzern ab. Service Grids werden von bestimmten IT-Dienstleistern wie Sun oder IBM angeboten.

Information Grids

Ein Information Grid schließlich als dritter Gridtyp liefert lediglich Daten. Das Internet mit den darauf aufsetzenden Diensten wie WWW, FTP usw. kann als universelles und omnipotentes Information Grid betrachtet werden, wobei die Informationen beispielsweise HTML-Seiten, CGI-Skripte oder Files sein können. Die folgende Abbildung zeigt den Zusammenhang zwischen Resource Grid, Service Grid und Information Grid noch einmal grafisch auf.



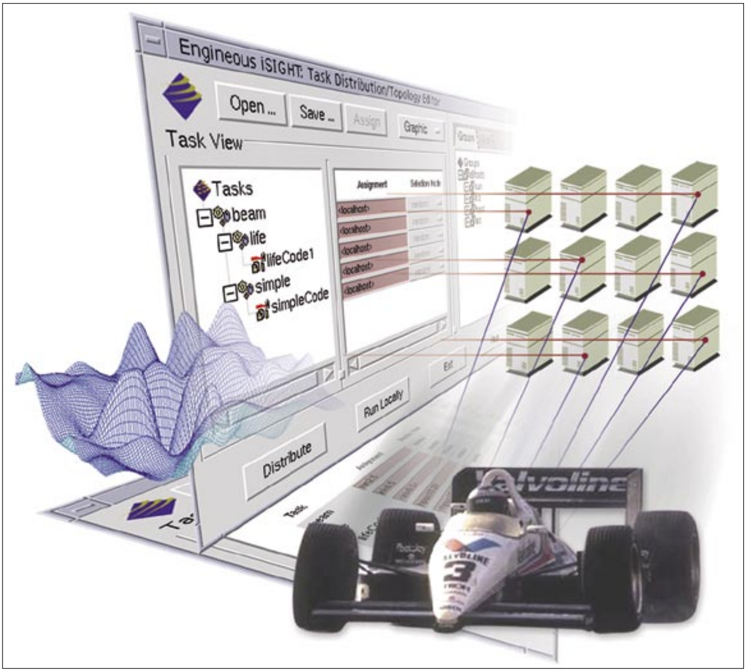
Die drei Grid-Typen im Überblick: Resource Grids, Service-Grids und Information Grids. (Quelle: ZIB Berlin)

Grid Computing erlebt derzeit einen regelrechten Boom. Eine ganze Reihe von wissenschaftlichen und Industrie-Projekten befasst sich mit diesem Thema. So will zum Beispiel das vom Bundesministerium für Bildung und Forschung geförderte Projekt D-Grid (www.d-grid.de) eine deutsche Grid-Infrastruktur schaffen. Weitere Grid-Initiativen finden Sie beim Bundesministerium für Bildung und Forschung (BMFW, www.e-science-forum.de/de/111.php).

Eine ausführliche, sehr übersichtliche deutschsprachige Liste mit Grid-Projekten aus verschiedenen Wissenschaftsdisziplinen finden Sie unter http://217.160.138.71/wiki/index.php?title=Projekt%C3%Bcbersicht. Auch Software-Konzerne wie beispielsweise IBM, Sun und Oracle betreiben Grid-Projekte.

1.4.12 Distributed Computing

Recht fließend geht Grid Computing in Distributed Computing (DC) über. Beim „Verteilten Rechnen“ delegiert ein zentraler Server Rechenaufgaben auf mehrere, unter Umständen weltweit verteilte Clients. Aus den Teilergebnissen ermittelt ein Zentralrechner das Gesamtergebnis.



Distributed Computing: Eine rechenintensive Aufgabe wird auf mehrere Clients aufgeteilt.

DC und Computational Grids sind eng verwandt. Gelegentlich werden beide Begriffe auch als synonym behandelt, denn in beiden Fällen geht es vorrangig um die Verteilung von Rechenleistung. DC-Projekte nutzen allerdings in der Regel eigene Protokolle, die weder offen noch standardisiert sind und auf den speziellen Zweck zugeschnitten sind. Zudem läuft DC immer über eine zentrale Instanz, die die Aufgaben verteilt und die Ergebnisse wieder zusammensetzt.

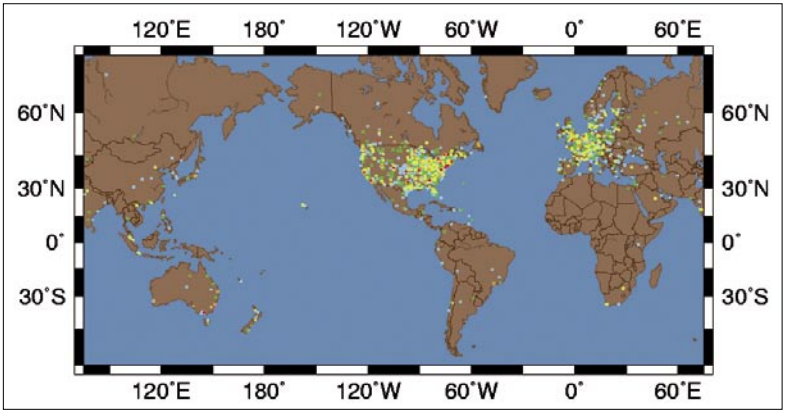
1.4.13 Distributed Computing: Prinzip

Für gewöhnlich wird für Distributed Computing das Internet als Kommunikationsmedium genutzt. Die populären Projekte gehen dabei nach folgendem Prinzip vor: Jeder Netzuser, der Interesse hat, kostenlose CPU-Leistung seines Rechners zu spenden, lädt die Projekt-Software herunter und installiert sie auf seinem PC. Das Programm läuft im Hintergrund und bedient sich des Rechners nur dann, wenn CPU-Leistung zur Verfügung steht – wenn also der PC gerade nicht oder nur mäßig benutzt wird.

Während dieser Zeit bearbeitet der Rechner eine einzelne Teilaufgabe des Projektes. Nach der Fertigstellung dieser Teilaufgabe wird das Ergebnis per Internet an den Zentral-Server geschickt, der die Teilberechnung auswertet und in den Gesamtprozess integriert. Nach Empfang der Daten übergibt der Zentral-Server dem Programm auf dem teilnehmenden Rechner eine neue Aufgabe per Datenleitung. In der Regel wickelt das Client-Programm die komplette Verarbeitung selbständig ab, einschließlich Wiederaufnahme der Berechnung bei Unterbrechung und Übermittlung des Ergebnisses.

1.4.14 Distributed Computing: Projekte

Verteiltes Rechnen hat vor allem im wissenschaftlichen Bereich Einzug gehalten. Eines der ersten Projekte, das die Technik des verteilten Rechnens nutzte, war SETI@home (http://setiathome.ssl.berkeley.edu) von der University of California. SETI@home sucht nach Signalen in radioastronomischen Daten, die von außerirdischen Intelligenzen stammen könnten und verwendet hierzu die ungenutzte Rechenleistung angeschlossener Internet-Clients.



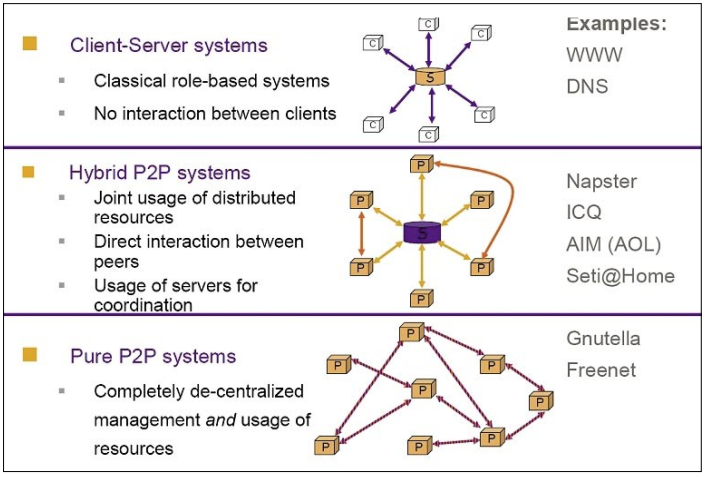
Weltweite Allianz: Seite Oktober 2000 haben mehr als 1.000.000 CPUs rund um die Welt an Folding@Home teilgenommen. (Quelle: Folding@Home)

Ein anderes populäres DC-Projekt ist Folding at home (http://folding.stanford.edu), bei dem die Faltung von Proteinen berechnet wird. Die Proteinfaltung und die Proteinaggregation sind sehr rechenintensive Vorgänge. Die entsprechenden Algorithmen werden in dem Projekt so verteilt, dass für jeden Computer, der an dem Projekt teilnimmt, eine angemessene Zunahme der Simulationsgeschwindigkeit erreicht wird. Ein drittes Beispiel ist das Krebsforschungsprojekt auf der Grid.org-Plattform (www.chem.ox.ac.uk/curecancer.html), welches in Zusammenarbeit mit dem Centre for Computational Drug Discovery der Oxford University sowie der National Foundation for Cancer Research (NFCR, www.nfcr.org) entstand, und bei dem nahezu drei Millionen PCs an der Sichtung von erfolgversprechenden Molekülen für Krebstherapeutika mitwirkten. Das laufende Projekt hatte bis Oktober 2005 mehr als 440.000 CPU-Jahre gerechnet.

Auch in Mathematik und Informatik hilft die Verteilung von Rechenleistung bei der Lösung von Problemen. „Global Internet Mersennee Prime Search“ (www.mersenne.org/prime.htm) sucht mit Hilfe von Distributed Computing nach der so genannten mersenneschen Primzahl, RC5-72 (www.distributed.net/rc5) will einen 72 Bit langen RC5-kodierten Schlüssel knacken.

1.4.15 Peer-to-Peer-Netzwerke

Seit Napster & Co. sind Peer-to-Peer-Netzwerke populär. Hinter dem Schlagwort Peer-to-Peer verbirgt sich aber mehr als nur die beliebten, aber zwielichtigen Filesharing-Systeme – nämlich Netzwerke, die auf den Prinzipien Dezentralität und Selbstorganisation aufbauen.



Übersichtlich: Reine und hybride P2P-Netze im Vergleich zu klassischen Client-Server-Architekturen. (Quelle: Stephan Fischer)

Peer-to-Peer-Netzwerke kommen grundsätzlich ohne zentrale Kontrollinstanz kommen aus – was sie von den anderen Verbundrechenarten grundlegend unterscheidet. Sie bestehen aus einem Netz gleichberechtigter Rechner, bei denen jeder Knoten gleichzeitig die Client- und Server-Rolle inne hat. Die Kommunikation erfolgt ohne Umwege direkt miteinander. Allerdings können P2P-Netze auch in hybrider Form existieren, bei denen die Teilnehmer mit einem zentralen Server kommunizieren. Diese zentral organisierten Systeme beinhalten entweder einen Discovery-Server, der beim Auffinden weiterer Peers hilft, oder aus einem Discovery- und Look-up-Server. Letzterer hält dabei eine Liste von Dateien im Netz vor, so dass das Suchen und Beziehen von Daten im Netz beschleunigt wird.

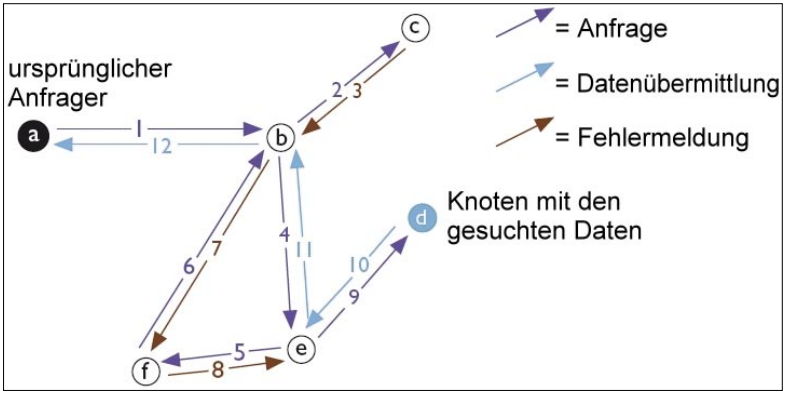
1.4.16 Vor- und Nachteile von P2P

P2P-Netzwerke versprechen im Vergleich zu klassischen Client-Server-Architekturen eine bessere Skalierbarkeit, niedrigere IT-Betriebskosten, selbstorganisierte und dezentrale Koordination von bislang unausgelasteten oder limitierten Ressourcen, höhere Fehlertoleranz sowie eine bessere Unterstützung spontaner Vernetzung und Kommunikation. Dem stehen als Nachteile gegenüber, dass bei P2P-Netzen die Zuverlässigkeit fehlt, eine zentrale Datensicherung unmöglich ist und die Administration nicht von Profis erledigt wird. Dafür erschließen sich durch P2P-Netzwerke neue Anwendungsszenarien, die mit herkömmlichen Ansätzen kaum praktikabel realisierbar sind. Derzeit beschränken sich existierende Anwendungen vor allem auf Filesharing und Zusammenarbeit (Collaboration).

Die aktuellen Filesharing-Projekte wie Gnutella und Kazaa basieren auf dem Konzept des rein dezentralen Peer-to-Peer und enthalten keine zentralen Server. Napster hingegen bestand ursprünglich aus einem hybriden Peer-to-Peer-Verbund. Dass sich ein rein dezentraler Ansatz hier durchgesetzt hat, hat einen einsichtigen Grund: Ein Netz ohne zentrale Instanz erschwert Überwachungsversuche und Zensur und begünstigt die Anonymität der Teilnehmer.

1.4.17 Collaboration

Neben Filesharing ist derzeit auch Collaboration eine Domäne von P2P-Netzen. Ein Beispiel, wie Zusammenarbeit auf P2P-Basis aussehen kann, ist das Freenet-Projekt (http://freenet.sourceforge.net), derzeit noch im Beta-Stadium. Freenet will Daten aller Art über das Internet anonym verbreiten. Jeder Rechner tritt dabei über eine frei erhältliche Java-Software dem dezentral organisierten Peer-to-Peer-Verbund bei. Neben der Veröffentlichung von Informationen eignet sich Freenet auch zur zeitversetzten Kommunikation, das heißt, sowohl E-Mail-Systeme als auch Diskussionsforen können sinnvoll auf Freenet aufbauen. Eine deutschsprachige Beschreibung des Projektes finden Sie unter www.freenethelp.org/html/DasFreenetProject.html.



Ablauf einer Anfrage in Freenet: Die Anfrage wird von Knoten zu Knoten durch das Netz geleitet, findet schließlich die gesuchten Daten und liefert diese zurück.

1.4.18 Fazit

Cluster, Grid, Distributed Computing und P2P Netzwerke setzen auf Vernetzung, haben ansonsten aber nicht viel gemeinsam. Distributed Computing hat vor allem im wissenschaftlichen Bereich seine Domäne, P2P-Netzwerke bilden derzeit die Infrastruktur von privaten Tauschbörsen, Cluster und Grids sind eher auf Unternehmensbedürfnisse zugeschnitten.

Die folgende Tabelle zeigt abschließend noch einmal im Überblick alle wesentlichen Parameter der vier Rechnerverbünde.

Cluster, Grid-, Distributed Computing und P2P im Vergleich				
	Cluster	**Grid**	**Distributed Computing**	**P2P**
Ziel	Hochverfügbarkeit, Rechenleistung, Lastverteilung	Integration und Nutzung verteilter Ressourcen	Verteiltes Rechnen, eine Zentrale verteilt die Aufgaben	Dezentraler Datenaustausch, Kommunikation und Zusammenarbeit
Verbindung	Ethernet oder Highspeed-Netze	Internet	Internet	Internet
Teilnehmer-Verteilung	Gebäude, Firmengelände	Weltweit	Weltweit	Weltweit

Während Cluster aber schon seit vielen Jahren etabliert sind, müssen Grids ihre Erwartungen erst erfüllen. Noch dominieren hier wissenschaftliche Anwendungen, doch Experten erwarten von der Technologie umwerfende Umwälzungen in der kommerziellen IT.

Dr. Klaus Manhart

tecCHANNEL-Links zum Thema	Webcode	Compact
Networked Computing: Grundlagen und Anwendungen	439222	S.42
Grid-Technologie Teil 1: Grundlagen, Dienste und Tools	435980	–
Grid-Technologie Teil 2: Grundlagen, Dienste und Tools	438803	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

1.5 Netzwerk-Tools für kleine und mittlere Windows-LANs

Zum Testen von Servern und zum Administrieren von Computern im Netzwerkverbund benötigen Systemverwalter immer wieder Spezialprogramme. Kleine kostenlose Tools stellen gegenüber den Windows-Bordmitteln erweiterte Funktionen zur Verfügung. Damit lassen sich etwa Überwachungs- und Fernsteuerungsaktionen durchführen, sodass der Administrator sein Netzwerk jederzeit unter Kontrolle hat. In diesem Artikel stellen wir eine Sammlung hilfreicher Netzwerk-Utilities für Windows-Systeme vor, die dem Administrator das Leben erleichtern. Die besten Programme finden Sie auch auf der Heft-CD konnten wir für Sie auf die Heft-CD packen.

1.5.1 Packet Sniffing

Systemverantwortliche setzen zur Fehlerdiagnose häufig einen Netzwerk-Sniffer ein. Diese Tools lauschen den Datenverkehr mit, speichert Transferprotokolle und erlauben eine Bit-genaue Analyse der Daten. Mit Sniffern kann man Fehler im LAN aufspüren, aber auch Programme, die Daten heimlich versenden. Profis investieren in einen guten Packet Sniffer durchaus mehrere Hundert oder Tausend Euro. Administratoren kleinerer und mittlerer Netze kommen oft auch mit Freeware-Sniffern weiter.

Traffic-Monitoring mit Wireshark

Eines der wenigen gut gemachten kostenlosen Tools zum Auswerten des Netzwerkverkehrs ist Wireshark 0.99.4. Das ehemals unter dem Name Ethereal entwickelte Tool setzt auf den kostenlosen Capture Driver Winpcap auf, der unter http://winpcap.polito.it zum Download bereitliegt. Winpcap klinkt sich in den Treiber des Netzwerkadapters ein und sorgt dafür, dass alle gesendeten und empfangenen Pakete in einem Puffer zwischengespeichert werden. Darauf greift Wireshark zu. Die Software erlaubt es, sowohl Daten im laufenden Netzwerkbetrieb zu analysieren, als auch archivierte Daten aus einer Protokolldatei zu lesen. Es lassen sich Details über jedes einzelne TCP/IP-Paket auf den Bildschirm bringen. Zusätzlich verfügt der Sniffer über Analyse- und Reportfunktionen sowie eine eigene Scriptsprache zum Filtern von Netzwerkpaketen. Das einzige Manko an Ethereal ist die umständliche Definition der Filter.

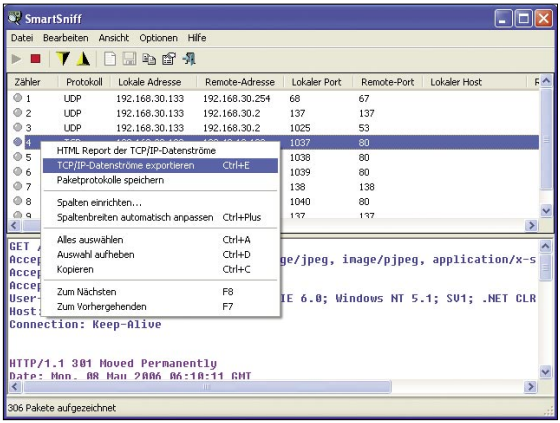
In Sachen Ausstattung übertrifft Colasoft Capsa 6.3 das Gratis-Tool Wireshark nur geringfügig, in Sachen Bedienkomfort liegt Capsa jedoch deutlich vorne. Mit der Software lassen sich Fehlerquellen aufdecken und Datenfragmente identifizieren. Umfangreichen Filtermechnismen mit individuellen Protokollregeln unterstützen den Administrator bei der Arbeit.

Sniffen vom USB-Stick aus

Auch mit einem auf das Wesentliche beschränkten Netzwerk-Sniffer wie SmartSniff 1.30 lassen sich alle Daten protokollieren, die durchs lokale Netz wandern. Dabei ist das Tool im Unterschied zu Wireshark nicht auf einen installierten Paketreiber angewiesen, unterstützt diesen aber. SmartSniff läuft ohne vorherige Installation und schneidet den über die Netzwerkkarte und einem lokalen Server oder einer Internet-Gegenstelle laufenden Datenverkehr mit. Damit eignet es sich für den direkten Start von einem USB-Stick.

Die Protokolldatei lassen sich im Hex-Format einsehen. Zusätzlich is ein Umschalten zum ASCII-Modus möglich. Letzterer eignet sich primär für Text-Protokolle wie HTTP, SMTP, POP3 und FTP an, die sich damit im Klartext interpretieren lassen.

TCP/IP-Monitoring: Der Packet Sniffer SmartSniff analysieren die übertragenen Netzwerkdatenpakete



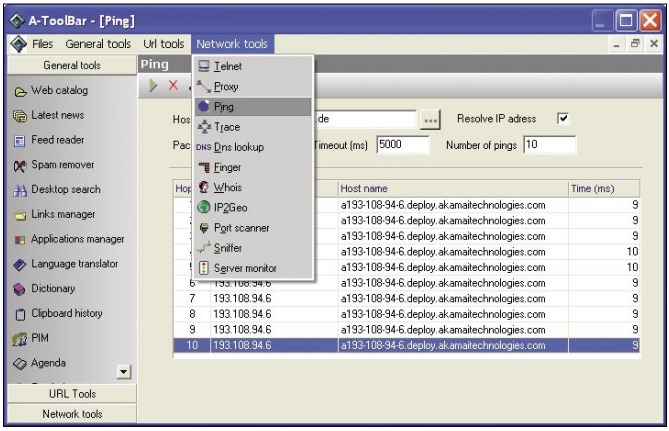
1.5.2 Verbindungskontrolle

Wenn Daten tröpfeln oder gar nicht über die Leitung laufen, bieten Bordwerkzeuge wie Ping und Traceroute erste Hilfe. Dabei handelt es sich allerdings nur um einfache Kommandozeilenprogramme, die über Parameter gesteuert werden müssen. Einige Gratis-Tools erfüllen einen ähnlichen Zweck wie die Bordwerkzeuge, verfügen jedoch über eine zeitgemäße grafische Bedienung und zusätzliche Funktionen.

Erreichbarkeits-Check mit der A-Toolbar

Der einfachste Weg, zu überprüfen, ob eine Website oder ein Server erreichbar ist, läuft über den Ping-Befehl. Mit Ping.EXE von Windows checken Sie die Netzwerkverbindung zu einer anderen Station. Ping ist damit vor allem für die Fehlerdiagnose interessant, denn es lassen sich nicht nur Rechner anpingen, sondern alle

Geräte, die über eine eigene IP-Adresse verfügen. Sobald eine Station auf Ping nicht reagiert, funktionieren alle anderen Netzwerkdienste mit dieser Gegenstelle nicht. Entweder liegt eine Hardware-Fehlfunktion vor, oder die entsprechenden Netzwerkeinstellungen sind fehlerhaft, oder eine Verständigung ist aufgrund unterschiedlicher Protokolle nicht möglich. Bei Web-, FTP- und Newsservern können Sie mit Ping herausfinden, ob der entsprechende Server überhaupt online ist.



Alles dabei: In der A-Toolbar stecken rund 50 Netzwerk-Tools, angefangen von Ping über Whois-Abfragen bis hin zu Wake on LAN

Komfortabler als mit Ping.EXE nutzen Sie Ping mit der A-Toolbar 3.01. Nach dem Programmstart klicken Sie auf den runden blauen Button, tippen die Adresse der zu überprüfenden Gegenstelle bei „Host“ ein und starten den Check mit der <Return>-Taste. Neben Ping hält die Auswahlleiste von AToolbar noch jede Menge weiterer Internet- und Desktop-Werkzeuge bereit. So bietet das Programm beispielsweise Portscanner, Adressabfragefunktion, Suchmaschinenmaske, DNS Lookup, Whois, Google Page Rank und einen Link Manager. Mit der Desktop-Suche können Sie auf dem Rechner nach Mails und Dokumenten recherchieren. Die Treffer zeigt das Tool unter „Result Tabs“ an. Die Startleiste der A-Toolbar siedelt sich über der Taskleiste auf dem Desktop an. Sie lässt sich bei Bedarf minimieren, so dass für Anwendungen die gewohnte Fläche zur Verfügung steht.

Query Application 1.06 und Etoolz

Nicht ganz so umfangreich wie A-Toolbar, dafür aber auf das Wesentliche beschränkt ist das englischsprachige Query Application 1.06. Mit dem Tool können Sie Server anpingen, den Domain-Namen zu einer IP ermitteln, nachprüfen, wer eine Domain angemeldet hat, und den Verbindungsstatus Ihres PCs ermitteln. Die Prüfresultate der insgesamt 15 Einzelmodule lassen sich als Textdatei speichern.

Wer ein möglichst einfaches IP-Checkprogramm sucht, greifen zum englischsprachigen Etoolz 3.0. Die Freeware enthält lediglich die wichtigsten TCP/IP-Prüfroutinen wie Ping, NS Lookup, Traceroute und Whois. Gut: Die Software unterstützt auch internationale Domain- Namen mit Umlauten.

Den Weg eines Datenpakets auflisten

Der Diagnosebefehl Tracert.EXE ermittelt die Route von Datenpaketen zu einem Ziel, indem er ICMP-Echopakete (Internet Control Message Protocol) sendet. Bequemer als in der Kommandozeile nutzen Sie Tracert mit 3D Traceroute 2.1.8. Größter Unterschied zum altbackenen Windows-Pendant: Die Freeware zeigt Ihnen die Wege durch das Internet anschaulich als Grafik an. Das vom Tool erzeugte Diagramm informiert Sie nicht nur über die Anzahl der Zwischenstationen, sondern auch über ihre Reaktionsgeschwindigkeit. Anhand der Grafik erkennen Sie auf einen Blick, ob Störungen auftreten und wenn ja, wo. Über zahlreiche Einstellmöglichkeiten richten Sie die Grafikausgabe nach Ihren Wünschen ein.

Visual Route 2007 11.0c setzt zwar auf nicht ganz so aufwendige 3D-Grafiken, dafür ist die Lesbarkeit der Diagramme ein Trick besser als bei 3D Traceroute. Auch bei diesem Tool gibt der Nutzer einfach eine URL oder IP-Adressse ein, und kurz Zeit später zeigt Visual Route, über welche Stationen die Pakete laufen. Zu den einzelnen Stationen liefert das Tool ausführliche Infos.

1.5.3 Administrationshelfer

Ganz gleich, wie groß ein Netzwerk ist und wie viele Anwender damit arbeiten – mit den richtigen Utilities ausgestattet geht die Administration leichter.

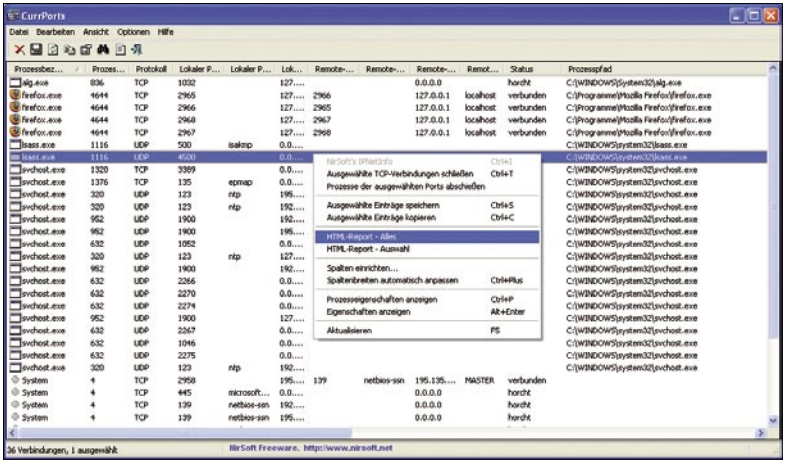
Informationen im Netz sammeln

Mit AdvancedRemoteInfo 0.6.5.4 sammeln Administratoren ausführliche Informationen über Windows-Arbeitsstationen. Anschließend kann zu jedem PC ein Bericht angezeigt werden. Der Report enthält unter anderem eine Auflistung der vorhandenen Hard- und Software, der derzeit angemeldeten Benutzer und die Netzwerk- Konfiguration auf PCs mit Windows NT, 2000 oder XP. Die von der Freeware erfassten Daten lassen sich zur weiteren Bearbeitung im Excel oder HTML-Format exportieren. Darüber hinaus sind weitere Funktionen vorhanden. Beispielsweise lassen sich auf entfernten Rechnern Dateifreigaben löschen oder neue Shares anlegen. Der Systemverwalter kann zudem die Deinstallation von Programmen auf einem Remote-PC, das Herunterfahren oder Neustarts lassen sich über das Netzwerk veranlassen.

Überblick über offene Ports verschaffen

Nicht schaden kann es, in regelmäßigen Abständen zu überprüfen, welche Ports auf den Clients geöffnet und in Benutzung sind. Gut dafür geeignet ist CurrPorts 1.11. Sie starten das Tool und weisen die Software an, die insgesamt Ports des

Rechners zu checken und Ihnen mitzuteilen, welche Programme welche Ports mit welchen Protokollen nutzen. Weil die Auflistung auch versteckte Prozesse anzeigt, sind Rückschlüsse auf verborgene Malware möglich.



Portfreigaben auflisten: Bei der Suche nach den möglichen Verursachern vom Tempoeinbußen leistet die Freeware CurrPorts gute Dienste

Plattformunabhängiges Remote Control

Für die PC-Fernsteuerung existiert in der täglichen Praxis eine Vielzahl von Anwendungsmöglichkeiten. Einer der klassischen Schwerpunkte ist neben der standortübergreifenden Serveradministration der Zugriff auf Informationen von unterwegs. Mobile Anwender nutzen per Notebook den Arbeitsplatz-Computer und arbeiten mit den gewohnten Programmen und Daten. Flexibler beim Fernzugriff sind Administratoren mit der Open-Source-Steuerung VNC (Virtual Network Computing). Das Client-Programm ist klein und lässt sich ohne vorherige Installation von einem USB-Stick starten. Servermodule für den Host-PC gibt es für Windows, Linux und Mac OS, VNC-Clients existieren darüber hinaus auch für Pocket-PCs/PDAs und als Java-Applet für die Fernsteuerung im Browser.

Derzeit buhlen drei kostenlose VNC-Programme um die Gunst der Nutzer: RealVNC (www.realvnc.com) ist der Nachfolger des VNC-Originalprogramms und in Sachen Übertragungstempo nicht mehr auf dem aktuellen Stand. Bei TightVNC (www.tightvnc.com) handelt es sich um den großen Bruder von RealVNC mit eingebauter Datenkomprimierung für eine Beschleunigung des Bildschirmaufbaus. Parallel dazu wird UltraVNC (http://ultravnc.sourceforge.net) entwickelt, das über eine Reihe von Erweiterungen und Plug-ins verfügt. Kompatibel sind alle zueinander, denn sie basieren jeweils auf dem ursprünglichen VNC. Einzig UlraVNC bringt die erforderliche Verschlüsselung des Datenverkehrs mit.

Remotezugriff auf Daten

PuTTY 0.59 ist ein empfehlenswertes Terminal-Programm für SSH- und Telnet-Sessions mit konfigurierbaren Funktionstasten. Die Freeware Tool ersetzt das unsichere Telnet und bietet Verschlüsselungs- und Authentisierungsverfahren für den Remote-Zugriff auf einen Rechner im LAN oder über das Internet.

Ebenfalls in den Werkzeugkoffer von Administratoren gehört WinSCP 3.8.2. Der Open-Source-SFTP-Client mit grafischer Oberfläche nutzt das SSH-Protokoll und lässt sich komfortabel wie ein FTP-Client verwenden. Zu den Extras gehören neben dem geschützten Dateitransfer die Funktionen Stapelverarbeitung, Kommandozeileneingabe, integrierter Text-Editor und Verzeichnissynchronisation.

1.5.4 Nützliche Tools

In einem lokalen Netzwerk gibt es stets etwas zu optimieren. Free- und Shareware-Tools sowie Programme kommerzieller Anbieter erleichtern dem Administrator den Alltag und erweitert Windows um zusätzliche Netzwerkfunktionen.

Gesperrte Dateien freigeben

Manchmal wird der Löschversuch für eine Datei mit einer Fehlermeldung quittiert, weil das betreffende Element gesperrt ist. Erst nach einem Neustart ist die Blockade aufgeboben – zumindest in einigen Fällen. Abhilfe schafft die Freeware Unlocker 1.7.2, die sich nach der Installation in das Kontextmenü des Explorers einklinkt. Nach der Auswahl einer gesperrten Datei oder eines Verzeichnisses rufen Sie über die rechte Maustaste den Eintrag *Unlocker* auf und klicken auf die Schaltfläche *Unlock*. Danach ist das Element entsperrt kann gelöscht werden.

Rechtevergabe vereinfachen

Microsoft Shared Computer Toolkit für Windows XP (Suche auf www.microsoft.com) erleichtert dem Administrator die Konfiguration von Benutzer-Rechten auf Windows-XP-Rechnern. Geeignet ist das Tool vor allem für PCs, die abwechselnd von unterschiedlichen Anwendern genutzt werden. Über die englischsprachige Bedienerführung lassen sich beispielsweise die Systemsteuerung sperren oder Änderungen am Startmenü unterbinden. Außerdem kann der Admin das Ausführen unbekannter Software blockieren und den Zugriff auf wichtige Daten reglementieren. AmRechner vorgenommene Änderungen können auf Wunsch bei jedem Neustart gelöscht werden. Gut: Ein Assistent führt in acht Schritten durch die wichtigsten Einstellungen, die sichmit einem Klick dauerhaft sichern lassen.

Hardware-Eigenschaften anzeigen

AdapterWatch 1.01 liefert Statusinformationen zu Netzwerkinterface. Zu den vom Tool angezeigten Daten gehören unter anderem IP-Adresse, MAC-Adresse, DNS, die Anzahl der übertragenen Pakete, Übertragungstempo und Paketstatistiken.

Dienste und Verzeichnisse überwachen

Mit FS Guard 3.2 können Administratoren Dienste und Ordner auf NT/2000- und 2003-Servern automatisch überwachen. Dazu sind die zu überwachenden Elemente auszuwählen. So ist es möglich, permanent kritische Dienste auf dem Server zu observieren und gestoppte oder nicht mehr funktionierende Services neu zu starten. Das Programm kann Benachrichtigungen per Mail verschicken

Ramon Schwenk

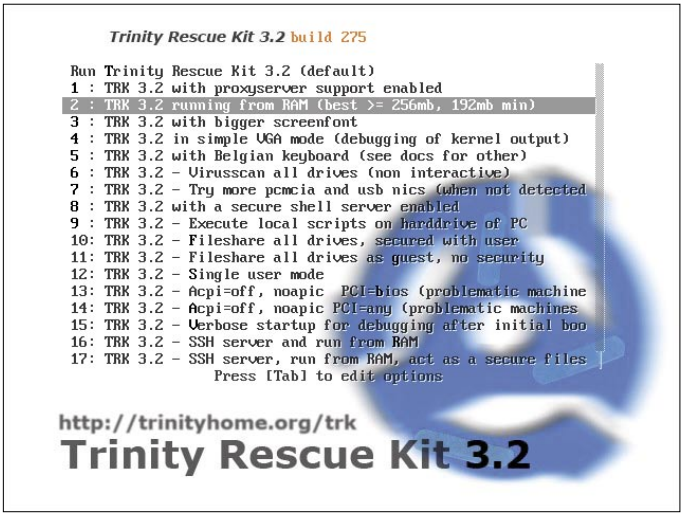
Netzwerk-Tools im Überblick

Programm	Lizenz	Sprache	Web
A-ToolBar 3.01	gratis	englisch	www.metaeureka.com
Query Application 1.06	gratis	englisch	www.leeos.com
AdvancedRemoteInfo 0.6.5.4	gratis	deutsch	www.masterbootrecord.de
Colasoft Capsa 6.3	ab 150 US-Dollar	englisch	www.colasoft.com
CurrPorts 1.11	gratis	deutsch	www.nirsoft.net
UlraVNC 1.02	gratis	deutsch	www.uvnc.com
PuTTY 0.59	gratis	englisch	www.chiark.greenend.org.uk/~sgtatham/putty/
WinSCP 3.8.2	gratis	deutsch	http://winscp.net
Unlocker 1.7.2	gratis	englisch	http://ccollomb.free.fr/unlocker/
Microsoft Shared Computer Toolkit	gratis	englisch	www.microsoft.com
AdapterWatch 1.01	gratis	deutsch	www.nirsoft.net
FS Guard 3.2	gratis	deutsch	www.pc-inspector.de
Wireshark 0.99.4	gratis	englisch	www.wireshark.org
SmartSniff 1.30	gratis	deutsch	www.nirsoft.net
3D Traceroute 2.18	gratis	deutsch	www.d3tr.de
Visual Route 2007 11.0c	ab 50 US-Dollar	englisch	www.visualware.com
Etoolz 3.0	gratis	englisch	www.gaijin.at

tecCHANNEL-Links zum Thema	Webcode	Compact
Netzwerk-Tools für kleine und mittlere Windows-LANs	461560	S.58

1.6 Erste Hilfe nach dem Crash: Trinity Rescue Kit

Das Linux-Live-System Trinity Rescue Kit (http://trinityhome.org/trk/) stellt verschiedene Erste-Hilfe-Werkzeuge bereit. Mit diesen können Sie versuchen, Ihren PC wieder herzustellen oder zumindest, die Daten zu retten. Die Distribution deckt eigentlich alles ab, was Sie dazu benötigen. Dazu gehören Virenscanner, Samba-Server, SSH-Verbindungen und ntfs-3g. Mit Letzterem können Sie auf NTFS-Partitionen lesend und schreibend zugreifen.

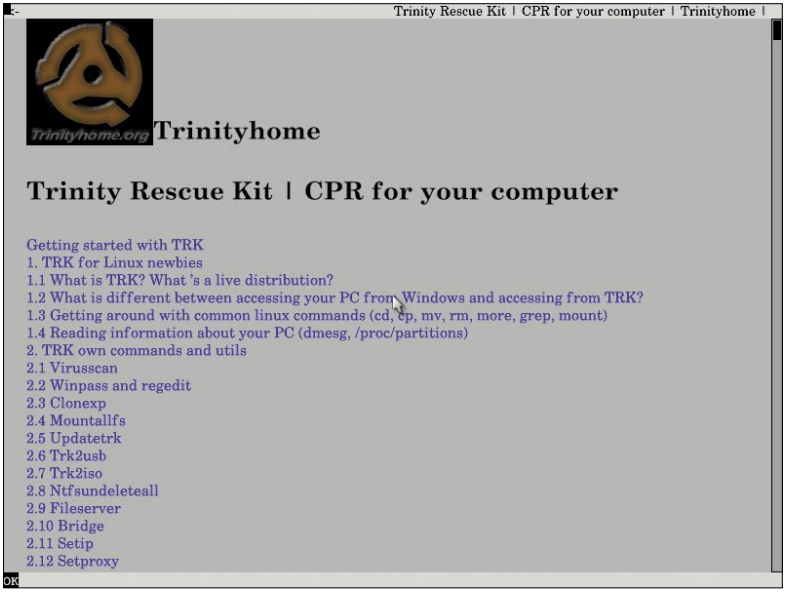


Verwirrend: Die Vielzahl der Auswahlmöglichkeiten ist auf den ersten Blick verwirrend, macht aber bei genauerem Hinsehen durchaus Sinn.

Der erste Start von Trinity Rescue Kit mag Unvorbereiteten etwas verwirrend erscheinen. Gleich 19 Bootoptionen stehen zur Auswahl. Für den Anfang sollte jedoch die Standardoption genügen. Hat Ihr Rechner mindestens 192 MByte RAM, käme Bootvariante „2“ noch in Frage. Hier lädt sich das komplette Betriebssystem in den Arbeitsspeicher und es lässt sich schneller damit arbeiten.

1.6.1 Grundsätzliches zur Distribution

Nach dem Start kommt man sich zunächst ein bisschen verlassen vor. Es blinkt ein Cursor auf der Kommandozeile und in großen Buchstaben ist noch Trinity Rescue Kit zu lesen. Die Linux-üblichen Manpages sind nicht vorhanden.



Hilfe naht: Weiß man nicht mehr weiter, gibt ein Blick in die Dokumentation Aufschluss.

Doch die Distribution bringt eine Hilfe-Datei mit sich. Wenn Sie Verbindung zum Internet haben, können Sie den Befehl `trkhelp` verwenden. Die Hilfe ist aber auch lokal vorhanden. Diese erreichen Sie mit `trkhelp -l`. Nun öffnet sich der Browser Links im grafischen Modus und gibt Ihnen die gewünschten Informationen. Beenden können Sie Links mit „q“. Der Entwickler gibt an, dass sich die Dokumentation an Nutzer richtet, die etwas Erfahrung mit PC-Troubleshooting haben. Zumindest sollten Sie wissen, wie Sie das eigene Windows installieren.

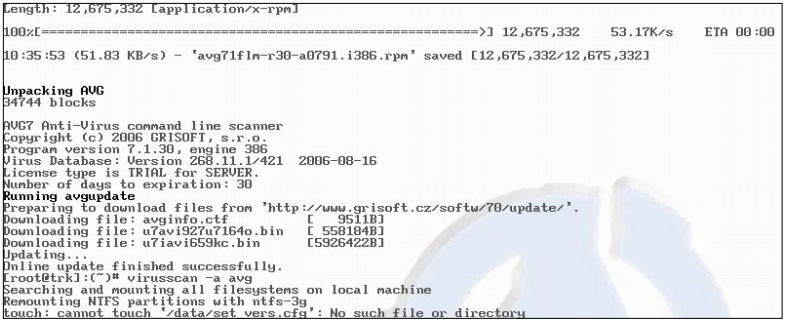
Weiterhin stellt Ihnen TRK insgesamt sechs verschiedene Konsolen bereit. Somit können Sie parallele Arbeitsabläufe starten, beispielsweise den Kopierprozess gewisser Dateien anstoßen und gleichzeitig nach weiteren zu sichernden Verzeichnissen Ausschau halten. Die unterschiedlichen Konsolen erreichen Sie mit ALT+<F1>-<F6>.

1.6.2 Die Werkzeuge von TRK

Die Virenscanner

Es stehen insgesamt vier verschiedene Virenscanner zur Verfügung. Sie können zwischen Clamav, F-Prot, Grisoft AVG und BitDefender wählen. Jeder dieser Scanner hat laut dem Entwickler der Distribution Vor- und Nachteile. Der persön-

liche Favorit des Entwicklers ist Grisoft AVG. Dieser Virenscanner erkennt am meisten Schadcode und ist schnell. Als Nachteile gibt er einen umfangreichen Download und die Notwendigkeit von viel Arbeitsspeicher an. Der Rechner sollte mindestens 256 MByte RAM aufweisen.



Gib Viren keine Chance: Virenscanner auf einer tragbaren Live-CD können ein wertvolles Werkzeug darstellen.

Das Schöne an der Sache ist, dass Sie alle vier Virenscanner mit einem einzigen Aufruf und den entsprechenden Optionen erreichen können: `virusscan -a <clam, avg, fprot, bde> -c -g -n -d <Zielort>`

Parameter für den Virenscanner	
Option	**Wirkung**
-a	Damit geben Sie an, welchen Virenscanner Sie verwenden möchten. clam – ClamAV, avg – Grisoft AVG, fprot – F-Prot, bde – BitDefender. Geben Sie diese Option nicht an, verwendet die Software als Standard ClamAV.
-c	„Use Common Extensions“: Nur gebräuchliche Dateiendungen scannen. Diese Option funktioniert nur mit ClamAV und beschleunigt den Scan-Prozess.
-g	„Get Only“: Hiermit laden Sie die neuesten Viren-Patterns nur herunter. Ein Virus-Scan wird hinterher nicht ausgeführt.
-d	„Destination“: Zu untersuchender Zielordner. Hier können Sie auch mehrere Ordner angeben. Diese müssen mit einem Komma getrennt sein. Verwenden Sie diese Option nicht, scannt TRK alle lokalen Dateisysteme, die es finden kann.
-n	„No Update“: Damit prüft die Software nicht nach den neuesten AntiVirus-Signaturen.
-h	Zeigt eine Hilfedatei an.

Zum Beispiel scannt der Aufruf `virusscan -g avg` alle gefundenen lokalen Festplatten. Sollte eine Partition noch nicht gemountet sein, geschieht dies automatisch. Nach dem Herunterladen von Grisoft AVG müssen Sie noch die angegebene Lizenznummer eingeben. Danach legt der Scanner los.

winpass und regedit

Mit winpass können Sie die Passwörter der vorhandenen Benutzer auf dem System zurücksetzen oder ändern. Rufen Sie das Tool ohne Optionen auf, benutzt es automatisch das Konto „Administrator“. Auf Windows-2000- und -XP-Systemen ist normalerweise Syskey aktiviert. Damit sind die Windows-Passwörter stärker verschlüsselt. Sie könnten dies mit winpass deaktivieren. Allerdings sollten Sie davon die Finger lassen. Damit werden alle Passwörter auf dem System ungültig und auf Windows 2000 lässt sich Syskey nicht wieder aktivieren. Ebenso könnte die Produktaktivierung für XP-Systeme ungültig werden. winpass ermutigt Sie sogar, Syskey nicht zu deaktivieren.

Ansonsten ist die Benutzung von winpass denkbar einfach. Zum Beispiel würde `winpass -u testuser` das Passwort des Benutzers „testuser“ ändern. Zunächst gibt Ihnen das Tool noch eine Liste aller gefundenen Windows-Installationen und Sie können auswählen, welche Sie verwenden wollen. Danach steht einer Passwortänderung nichts mehr im Wege. `winpass -l` listet alle angelegten Anwender auf und `winpass -h` zeigt Ihnen eine Liste aller vorhandenen Optionen.

```
Minimum password length        : 0
Password history count         : 0
RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <HelpAssistant>, *disabled or locked*
RID: 03eb, Username: <singh>
RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

----------------------> SYSKEY CHECK <-------------------------
SYSTEM   SecureBoot            : -1 -> Not Set (not installed, good!)
SAM      Account\F             : 1 -> key-in-registry
SECURITY PolSecretEncryptionKey: 1 -> key-in-registry

***************** SYSKEY IS ENABLED! **************
This installation very likely has the syskey passwordhash-obfuscator installed
It's currently in mode = -1, Unknown-mode
SYSKEY is on! However, DO NOT DISABLE IT UNLESS YOU HAVE TO!
This program can change passwords even if syskey is on, however
if you have lost the key-floppy or passphrase you can turn it off,
but please read the docs first!!!

** IF YOU DON'T KNOW WHAT SYSKEY IS YOU DO NOT NEED TO SWITCH IT OFF!**
NOTE: On WINDOWS 2000 it will not be possible
to turn it on again! (and other problems may also show..)

NOTE: Disabling syskey will invalidate ALL
passwords, requiring them to be reset. You should at least reset the
administrator password using this program, then the rest ought to be
done from NT.

Do you really wish to disable SYSKEY? (y/n) [n] n
RID      : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 0

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: _
```

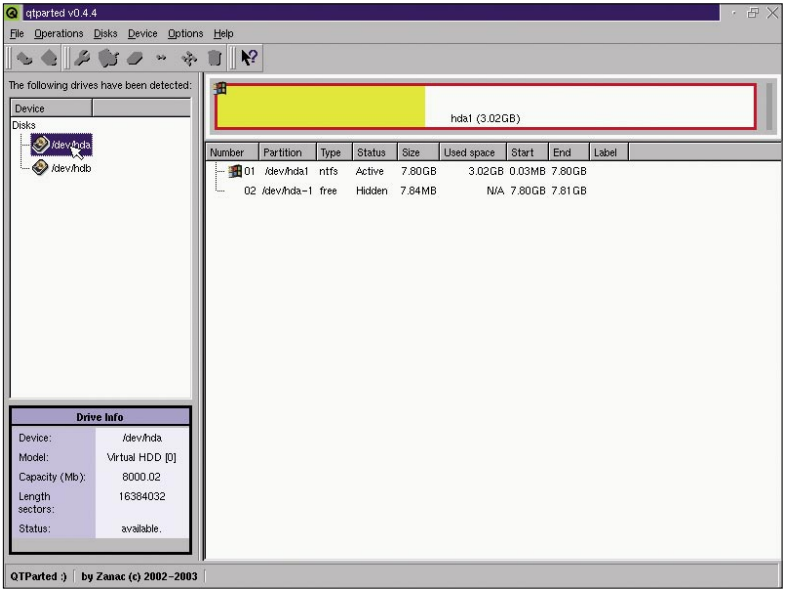
http://www.trinityhome.org/trk
Trinity Rescue Kit 3.2

Passwort vergessen? Mit winpass im Gepäck können Sie es sich erlauben, vergesslich zu sein.

regedit basiert auf dem gleichen Script wie winpass. Doch es kopiert alle „Registry Hives“ und öffnet diese. Dazu gehören SAM, Security, System und Software. Das Tool weiß nur nicht, welche Anwender-Registry es öffnen soll. Wer es benutzen möchte, findet Genaueres in der Dokumentation unter http://home.eunet.no/pnordahl/ntpasswd/.

NTFS-Partitionen mit CloneXP klonen

Dieses Werkzeug kann eine NTFS-Partition übers Netzwerk auf eine Festplatte eines anderen Rechners klonen. Dazu müssen allerdings beide Rechner mit TRK gebootet sein. Der Empfänger muss den SSH-Daemon aktiviert haben. Dies erreichen Sie mit der Bootoption 8: TRK 3.2 with a secure shell server enabled. Selbstverständlich muss die Empfängerpartition mindestens genauso groß sein wie die Senderpartition. Sollte dies nicht der Fall sein, hilft das implementierte Partitionswerkzeug `qtparted` weiter.



Erinnert an PartitionMagic: Das grafische Hilfsprogramm qtparted erweist sich als überaus nützlich beim Partitionieren von Festplatten.

CloneXP hat zwei Modi: Ohne Optionen aufgerufen, fragt das Tool nach den entsprechenden Daten. Sie können diese aber auch direkt übergeben. Zum Beispiel klont `clonexp /dev/hda1 192.168.1.100:/dev/sdb1` die erste Partition der IDE-Festplatte im Quell-Rechner auf die erste Partition der zweiten SCSI-

Festplatte des Ziel-Rechners. Letzterer hat in diesem Fall die IP-Adresse 192.168.1.100. Weiterhin steht die Option --bkupbr zur Verfügung. Dies kreiert eine Kopie des Bootrecord, speichert sie in eine Datei und legt sie dann auf der Ziel-Festplatte ab.

mountallfs: Alle gefundenen Massenspeicher einbinden

mountallfs erweist sich als nützlich, wenn man nicht alle integrierten Massenspeicher händisch einbinden möchte. Das Tool sucht nach lokalen Festplatten, USB-Sticks und so weiter und bindet diese unter dem Namen der Gerätebezeichnung ein. Zum Beispiel findet sich /dev/hda1 unter /hda1 wieder oder /dev/sdb2 unter /sdb2. Sollten Sie sich nicht sicher sein, ob das eine oder andere Gerät eingebunden ist, hilft eine Eingabe des Befehls `mount` weiter. Dieser listet Ihnen die derzeitige Mount-Tabelle auf.

Das Werkzeug bringt noch einige Optionen mit sich, die erwähnenswert sind. Ohne Parameter aufgerufen, verwendet das Tool den Kernel-integrierten Treiber für NTFS-Systeme. Dies gibt Ihnen zwar vollen Lesezugriff, jedoch nur eingeschränkten Schreibzugriff. Hilfreicher ist die Verwendung der Option -g. Damit bindet mountallfs NTFS-Partitionen mittels des ntfs-3g-Treibers ein. Somit haben Sie vollen Lese- und Schreibzugriff auf Windows-Partitionen.

Die Option -c verwendet den Captive-Treiber und somit die Original-Windows-Treiber ntfs.sys und ntoskrnl.exe. Diese sind aus Lizenzgründen nicht auf der CD enthalten. Möchten Sie diese Option verwenden, müssen Sie `updatetrk` auf einem Rechner ausführen, der Windows XP SP2 installiert oder eine Internetverbindung hat. Erfahrungsgemäß neigt Captive-NTFS bei vielen Schreibzugriffen zum Abstürzen. Die empfehlenswerte Methode ist die Verwendung von ntfs-3g.

`mountallfs -l` aktiviert das „Logical Volume Management"-Modul, das zum Einbinden von Linux-Partitionen hilfreich ist. Fedora verwendet es zum Beispiel als Standardoption bei der Installation. Der Befehl `umountallfs` löst alle Bindungen eingebundener Massenspeicher. Dies brauchen Sie eventuell, wenn Sie `updatetrk` verwenden.

Mit updatetrk, trk2usb und trk2iso eine eigene TRK-Version erstellen

Mit updatetrk können Sie mehr oder weniger ein eigenes TRK basteln. Wenn Sie TRK auf einem System starten, auf dem Windows XP, 2000 oder NT installiert ist, können Sie updatetrk ohne weitere Optionen aufrufen. Dann verwendet es die Datei pagefile.sys, um temporäre Dateien abzulegen. Ist dies nicht der Fall, müssen Sie dem Script mit dem Argument -b sagen, wo es mindestens 250 MByte Platz findet. Diesen Platz benötigt das System, um sich neu aufzubauen.

Zunächst fragt Sie das Script, ob Sie Captive-NTFS verwenden wollen. Dies ist seit ntfs-3g eigentlich obsolet und Sie können es verneinen. Danach holt es die neuesten Virensignaturen für die Virenscanner, beziehungsweise installiert diese zuerst. Als Letztes kopiert es die Verzeichnisse /bin, /sbin, /etc und /lib in das neue Image. Alle Änderungen, die Sie hier vorgenommen haben, erscheinen in der ei-

genen Version. Danach legt es die neue ISO-Datei auf der Partition im Verzeichnis temp ab, wo es die Datei pagefile.sys gefunden hat. Mit der Option -i können Sie dem Script allerdings ein anderes Zielverzeichnis mitteilen. Das Script funktioniert nur, wenn sich die TRK-CD im Laufwerk befindet. Sollten Sie TRK ins RAM booten lassen, wirft es die CD aus. Sie müssten entweder im Standardmodus starten oder die CD manuell einbinden.

Eigenbau: Nach einem updatetrk haben Sie etwa aktuelle Virensignaturen in der ISO-Datei.

trk2iso kreiert eine ISO-Datei des momentan laufenden Trinity Rescue Kit. Es ist ähnlich zu updatetrk, holt sich aber keine Updates aus dem Internet. Die Datei finden Sie danach in dem Verzeichnis, in dem Sie das Script gestartet haben. trk2usb kopiert das Betriebssystem auf einen USB-Stick oder eine Festplatte. Danach könnten Sie das Rettungssystem auf einem USB-Gerät mitnehmen. Voraussetzung für den Einsatz ist, dass der zu rettende Rechner von USB starten kann.

Ntfsundeleteall und photorec

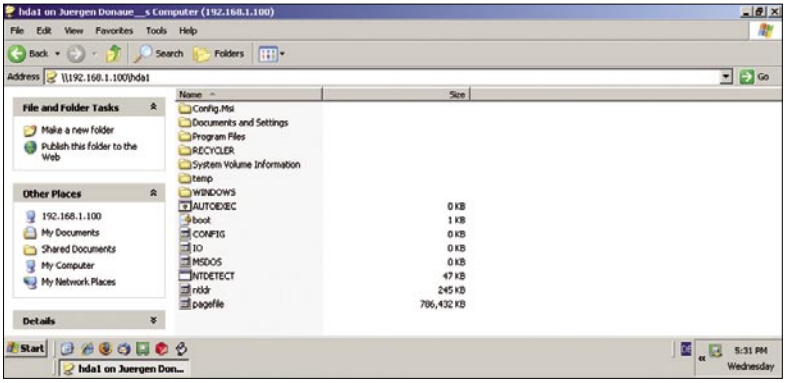
Dieses Helferlein ist ein „Wrapper“ für ntfsundelete. Es versucht, alle gelöschten Dateien auf einer NTFS-Partition zu finden und wieder herzustellen. Die zu durchsuchende Partition darf dabei nicht eingebunden sein. Weiterhin müssen Sie eine andere Partition für die wieder hergestellten Dateien definieren. Das Script schreibt keine Daten auf die zu durchsuchende Partition zurück. Es bestünde die Gefahr, andere gelöschte Dateien zu überschreiben. Beispielsweise würde `ntfs-`

`undeleteall /dev/hda1 /<andere Partition>/temp` alle wieder hergestellten Dateien nach <andere Partition>/temp sichern. Das Problem ist, dass genannter Aufruf alles wieder herstellt, was er finden kann. Wollen Sie nur Daten wiederhaben, die zu 100 Prozent vorhanden sind, hilft der Befehl `ntfsundeleteall /dev/hda1 /<andere Partition>/temp 100`.

Ein weiteres Werkzeug, um Daten wieder herzustellen, ist photorec. Dieses Tool ist dateisystemunabhängig. Es versucht weiterhin, bekannte Datenformate zu erkennen. Es ist allerdings nicht imstande, den originalen Dateinamen zu finden. Nach einer Rettungsaktion müssen Sie das händisch erledigen.

Datenserver mittels Samba

Der Aufruf `fileserver` startet Samba unter TRK. Damit könnten Sie von anderen Windows-Rechnern auf die eingebundenen Laufwerke zugreifen. Das Script beinhaltet zwei Optionen. Zum einen den sicheren Modus, den Sie mittels `fileserver -s` starten. Dieser Modus fragt den Anwender nach einem User und einem Passwort. Nur dieser User hat danach die Berechtigung, auf die eingebundenen Partitionen zuzugreifen. Der Gastmodus, `fileserver -g`, gibt jedem Benutzer im selben Netzwerk Zugriff auf die Daten. Sie sollten vor der Benutzung des Gastmodus überlegen, wie wichtig die Daten auf dem zu rettenden System sind.



Windows-Sharing: Mit dieser Methode könnten Sie auch Daten via Windows-PC kopieren.

Das Script ruft ebenfalls mountallfs -g auf. Danach verrät es die IP-Adresse, unter welcher der Samba-Server zu erreichen ist. Danach sollten Sie den TRK-Rechner im Netzwerk finden und auf die eingebundenen Partitionen zugreifen können.

Trinity Rescue Kit für Sniffing als „Bridge“ nutzen

TRK lässt sich mit dieser Funktion ebenfalls als so genannte Bridge einsetzen. Somit könnten Sie sich zwischen einen PC und zum Beispiel einen Switch schalten und den kompletten Netzwerkverkehr des Rechners untersuchen. Alles, was Sie

dafür brauchen, ist ein PC mit zwei Netzwerkkarten. Wichtig dabei ist, dass nur eine Netzwerkkarte eine IP-Adresse besitzt. Sollten beide eine haben, fahren Sie zum Beispiel Nummer zwei mit `ifconfig eth1 down` herunter. Danach rufen Sie den Bridge-Modus mit `bridge up` auf.

Nun könnten Sie mit `tcpdump -i eth0` das Sniffen beginnen. Somit sehen Sie jedweden Traffic, der von dem PC ausgeht. Um etwas spezieller zu filtern, hilft grep weiter. Wollen Sie zum Beispiel nur HTTP-Traffic sehen, würde der Befehl folgendermaßen aussehen: `tcpdump -i eth0 | grep http`. Sie können übrigens auch mehrere grep-Befehle hintereinander schreiben. Wollen Sie nur den HTTP-Traffic sehen, der zum Beispiel zur IP-Adresse 217.111.81.70 geht, verwenden Sie diesen Aufruf: `tcpdump -i eth0 | grep 217.111.81.70 | grep http`

setip und setproxy

`setip` ist relativ unspektakulär, kann allerdings nützlich sein. Damit weisen Sie einer bestimmten Netzwerkkarte eine fixe P-Adresse zu. Ein entsprechender Aufruf sähe zum Beispiel so aus: `setip eth0`. Das Script fragt nach der zu vergebenden IP-Adresse, Subnetzmaske, Default Gateway und DNS Server. Die beiden Letzteren sind optionale Angaben. Diese brauchen Sie allerdings, wenn Sie ins Internet wollen.

Netzwerkeinstellung fest vergeben: Mit dem Kommando setip lassen sich bei Bedarf bestimmten Netzwerkkarten fixe IP-Adressen zuweisen.

Mit `setproxy` können Sie TRK Proxy-Einstellungen mitteilen. Dies ist hilfreich, wenn Sie sich nicht direkt ins Internet verbinden können. Das Script fordert die IP-Adresse oder den Hostnamen des Proxy-Servers an, den Port und optional Benutzername und Passwort. Dieses Script könnte auch schon im Bootmenu aufgerufen werden. Folgende Applikationen verwenden danach die Proxy-Einstellungen: wget, links, ClamAV, F-Prot, Grisoft AVG und BitDefender.

1.6.3 Fazit

Trinity Rescue Kit sollte jeder Administrator im Gepäck haben, Gleiches gilt für den Heimanwender. Gewöhnungsbedürftig ist wohl für viele, dass sich im Prinzip alles auf der Kommandozeile abspielt. Dennoch ist es kein Hexenwerk, mit der Distribution umzugehen. Die Dokumentation ist relativ verständlich und beinhaltet kleine Beispiele. Der Entwickler hat sich sehr viel Mühe gegeben. Die bereitgestellten Werkzeuge sind intelligent gewählt und zeigen, dass professionelle Selbsthilfe nichts kosten muss. Somit steht Ihnen ein freies Rettungssystem zur Verfügung, das sich nach einem Crash als sehr nützlich erweist.

Es lohnt sich auf jeden Fall ein Blick in die Dokumentation (`trkhelp -l`). Dort kann der Anwender den einen oder anderen „Aha"-Effekt ergattern. Vor allen Dingen der dritte Punkt „Procedures" hilft weiter. Hier gibt der Entwickler wertvolle Tipps. Zum Beispiel finden Sie dort, wie sich eventuell Daten von sterbenden Festplatten retten lassen. Im Punkt 5 lesen Sie, wie Sie Trinity Rescue Kit via PXE aus dem Netzwerk heraus starten können.

Als Alternative zu TRK ist die SystemRescueCD (www.sysresccd.org) zu erwähnen. Auch hier schadet es nicht, eine Kopie zu haben. Dennoch kann das Trinity Rescue Kit etwas mehr und ist einfacher zu bedienen.

Jürgen Donauer

tecCHANNEL-Links zum Thema	Webcode	Compact
Erste Hilfe nach dem Crash: Trinity Rescue Kit	461110	S.65
Professionelle Datenrettung	401608	–
Linux-Partitionen: Tools für den Zugriff unter Windows	443178	–
Linux-Workshop: LiveCD selbst gemacht	438588	–
Bootfähige Rettungs-CD selbstgemacht	401534	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

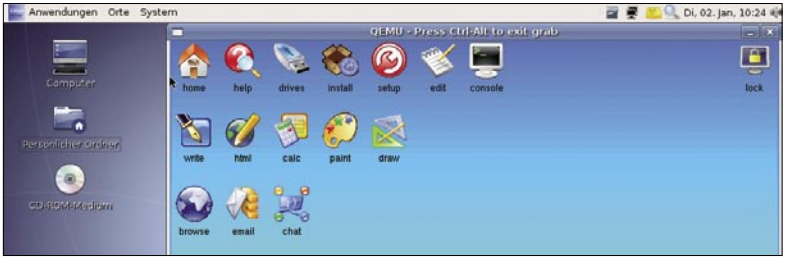
2. Linux / Novell Inside

Die Auswahl an Linux-Distributionen ist heutzutage riesig. Neben den großen und populären Zusammenstellungen gibt es eine Reihe von weniger bekannten Projekten, die zwar nur bestimmte Aufgaben erfüllen, diese jedoch besonders effizient. In diesem Kapitel geben wir einen Überblick über Spezialdistributionen. Das Spektrum reicht von einer Dank eingebautem Emulator direkt unter Windows startfähigen Live-CD-Distribution über Recovery- und Multimedia-Linuxe bis hin zum bootfähigen Festplattenpartitionierer auf Basis des Linux-Tools gparted. Zusätzlich geben wir Tipps zum Einsatz des NetWare-Dateisystems unter Linux.

2.1 QEMU-Puppy-Linux: Virtualisierung in der Hosentasche

Nicht immer hat man die Möglichkeit, eine Live-CD auf einem fremden Rechner zu booten. Wer dennoch „sein“ System verwenden will, kann auf die Kombination QEMU und Puppy Linux zurückgreifen. Puppy-Linux ist bekannt als schlankes, schnelles Betriebssystem, das auch älteren oder weniger leistungsstarken Rechnern neues Leben einhauchen kann. QEMU ist eine kostenlose Open-Source-Virtualisierung. Ein findiger Entwickler hat beides vereint und QEMU-Puppy erschaffen. Es passt auf einen USB-Stick und lässt sich in jedem anderen Linux oder Windows direkt als virtuelle Instanz starten.

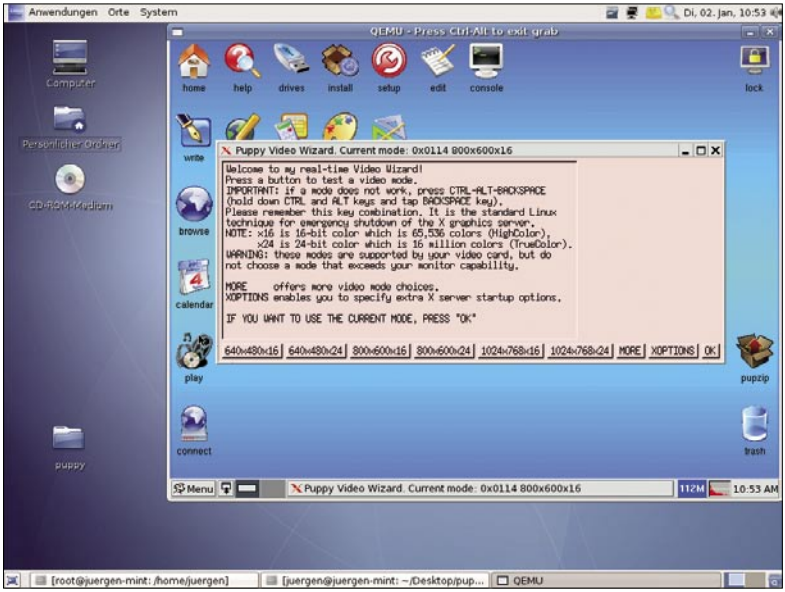
Somit haben Sie immer Ihr eigenes Betriebssystem dabei und brauchen nur einen anderen Rechner, um es zu starten. Dieser muss lediglich ein Linux oder Windows installiert haben – Sie müssen nicht einmal den Rechner booten. QEMU-Puppy enthält eigentlich alles, was man für unterwegs benötigt. Sie finden in der schlanken Distribution eine Textverarbeitung, einen Browser, ein E-Mail-Programm und vieles mehr. Veränderte Einstellungen und neue Dateien speichert das System auf dem USB-Stick. Diese sind beim nächsten Start wieder vorhanden. Das Gast-System bleibt dabei völlig unberührt – QEMU-Puppy hinterlässt keinerlei Spuren.



Mobiles OS: QEMU-Puppy können Sie auf jedem Linux- oder Windows-Rechner starten.

2.1.1 Herunterladen und Starten von QEMU-Puppy

Um QEMU-Puppy starten zu können, müssen Sie es logischerweise zunächst einmal herunterladen. Sie finden eine tar.gz-Datei auf sourceforge.net (https://sourceforge.net/project/showfiles.php?group_id=160696). Wahlweise können Sie es auch via BitTorrent beziehen (http://www.erikveen.dds.nl/qemupuppy/download/qemu-puppy-2.12-1.tar.gz.torrent). Auspacken können Sie die Datei unter Windows mit einem passenden Dekompressions-Programm (Winzip, 7-Zip und so weiter) oder unter Linux mit `tar xzvf <Datei.tar.gz>`.



Ansichtsache bei Puppy-Linux: Mit diesem Programm bestimmen Sie die Bildschirm-Auflösung des virtuellen Betriebssystems.

Ist das getan, lässt sich das Betriebssystem unter Windows mit `puppy.exe` starten. Unter Linux geschieht dies mit dem Befehl `./puppy.sh`. Beim ersten Start fragt das Betriebssystem nach einem Tastatur-Layout und welchen X-Server Sie verwenden möchten. Der Entwickler empfiehlt, immer den schlankeren Xvesa-Server zu verwenden.

Eigene Erfahrungen bestätigen, dass es damit die wenigsten Probleme gibt. Danach können Sie eine passende Bildschirm-Auflösung wählen. Solange Sie diese nicht mit „OK“ bestätigen, erscheint dieses Fenster bei jedem Neustart. Die Wahl von 16-bit-Farbtiefe könnte einen Tempovorteil bringen.

2.1.2 Virtualisierung beschleunigen

Für QEMU gibt es ein Beschleunigungs-Programm namens KQEMU. Das Programm beschleunigt die virtuelle Instanz erheblich. Möglich ist das, weil die Software viel Applikations-Code direkt im Host-Prozessor ausführt. Der Entwickler hat es nicht implementiert, da es laut eigener Aussage mit Vorsicht zu genießen ist. Er gibt drei Gründe an, warum es nicht in QEMU-Puppy enthalten ist.

- Ersten brauche man dann Administrator-Rechte, um das virtuelle Betriebssystem laufen zu lassen.
- Zweitens „verschmutze" das Laden des KQEMU-Moduls den Kernel des Host-Systems. Ziel von QEMU-Puppy sei es aber, das Host-System unberührt zu lassen.
- Drittens sei es lizenzrechtlich nicht möglich. Man könne sowohl die Datei *puppy.sh* als auch *puppy.exe* mit der Option *-kernel-kqemu* starten. Dies bringe noch mehr Performance. Wer es benutzen möchte sei gewarnt. Der Entwickler berichtet, dass er damit sein natives Windows mehrfach „geschrottet" hätte.

KQEMU unter Windows

Wer es trotzdem versuchen möchte, kann das Modul unter http://fabrice.bellard.free.fr/qemu/kqemu-1.3.0pre9.tar.gz herunterladen. In dem entpackten Verzeichnis befindet sich die Datei *kqemu.inf*. Diese installieren Sie mit Administratorrechten per Rechts-Klick. Nach einem Reboot des Systems starten Sie das Modul via Commandshell: `net start kqemu`. Das Modul muss nach jedem Neustart erneut geladen werden. Wer möchte, kann ein Script automatisch beim Hochfahren des Systems ausführen.

Beschleunigungsmöglichkeiten unter Linux

Für das Kompilieren von KQEMU unter Linux gibt es unter http://fabrice.bellard.free.fr/qemu/kqemu-doc.html eine Anleitung des Entwicklers. Sowohl QEMU als auch KQEMU sollten exakt gegen die gleiche Kernel-Version kompiliert sein. Die Datei *puppy.sh* erkennt sowohl das eigen kompilierte Kernel-Modul als auch das eigen erstellte QEMU und verwendet dies. Nach jedem Linux-Neustart muss man folgende Befehle als *root* ausführen:

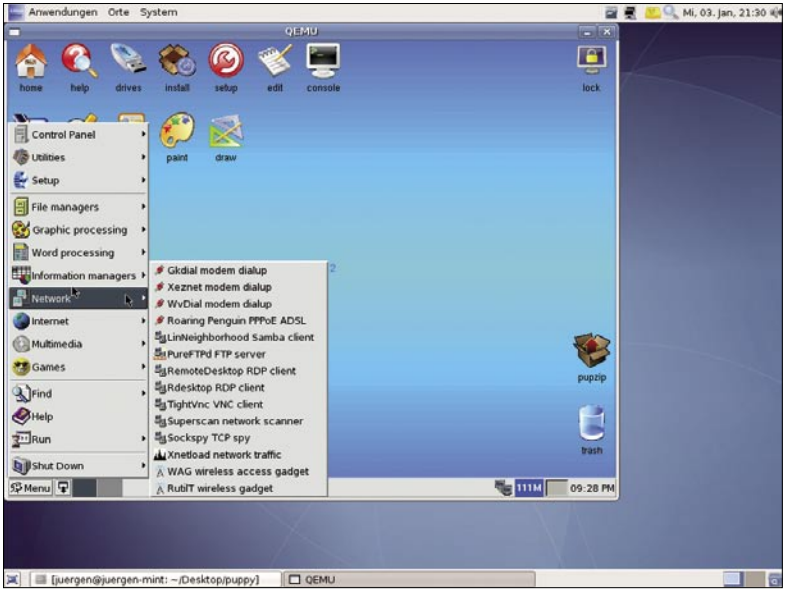
```
mknod /dev/kqemu c 250 0
chmod 666 /dev/kqemu
```

Wem das zu lästig ist, kann die Befehle in die Datei */etc/rc.local* eintragen. Somit startet das System das Kernel-Modul bei jedem Neustart automatisch. Einen weiteren Vorteil könnte der Befehl `echo 1024 > /proc/sys/dev/rtc/max-user-freq` bringen. Dafür müssen Sie ebenfalls *root* sein. Das Startscript weist Sie allerdings darauf hin, wenn es diesen Eintrag gerne hätte.

2.1.3 Applikationen in QEMU-Puppy

Das virtuelle Betriebssystem für Unterwegs bringt eigentlich alles an Applikationen mit, was man benötigt. So ist zum Beispiel die Internet-Suite SeaMonkey von Mozilla an Bord. Damit ist Internet-Browser, E-Mail-Programm und ein leistungsfähiges Adressbuch abgedeckt. Als Instant-Messenger steht ihnen Gaim zur Verfügung. Das gibt ihnen unter anderem Zugriff auf AOL/ICQ, Jabber, MSN, Yahoo, GroupWise und Napster. Abiword dient als Textverarbeitung und Gnumeric ist für Tabellenkalkulationen gedacht.

Auch die Sparte Multimedia-Anwendungen deckt Puppy-Linux ab. Hier finden Sie diverse Ripper und den Media-Player Gxine. Mit LinNeighborhood mangelt es auch an einem Samba-Client nicht. Für die Fernsteuerung anderer Rechner ist mit „Rdesktop RDP Client“ und „TightVnc VNC Client“ ebenfalls gesorgt.



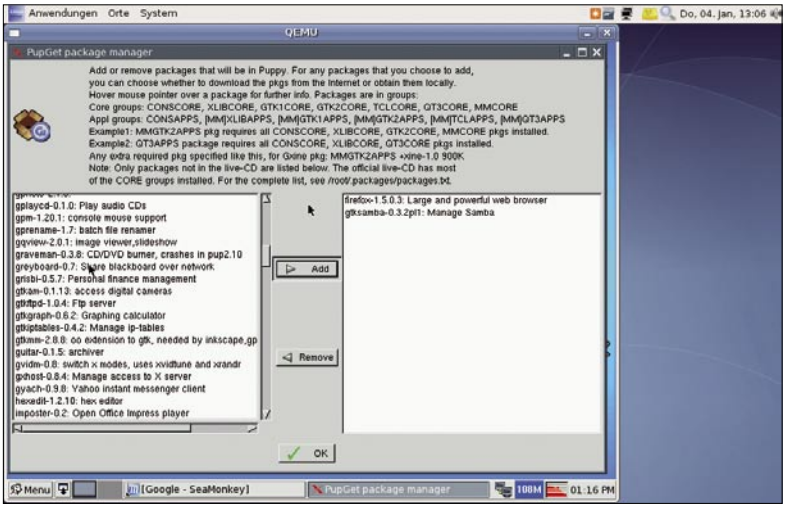
Reichhaltig: Trotz der Schlankheit von Puppy-Linux ist sehr viel nützliche Software an Bord.

Zusätzliche Software installieren

Möchten Sie zusätzliche Software installieren, finden Sie auf dem Desktop des Betriebssystems ein Icon „Install“. Somit gelangen Sie in den Puppy Package Manager. Als nützlich erweist sich hier der PupGet Package Manager. Er verbindet sich beim Aufrufen ins Internet und stellt ihnen eine Liste aller für Puppy verfüg-

baren Pakete bereit. Hier finden Sie eine weitere Auswahl an Software. Zum Beispiel stehen Firefox 1.5.0.3, gtksamba, Perl und sogar der Desktop-Manager GNOME zur Verfügung.

Die Bedienung ist denkbar einfach. Sie wählen die gewünschten Applikationen und fügen diese der Installationsliste hinzu. Der Paket-Manager löst ebenfalls alle Abhängigkeiten auf und installiert diese mit. Somit ist das Einspielen zusätzlicher Applikationen denkbar einfach.



Einfach: Das Installieren zusätzlicher Software aus dem Puppy-Pool ist ein Kinderspiel.

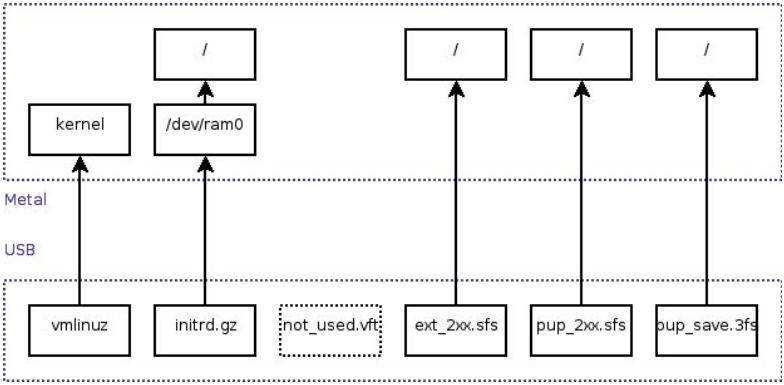
2.1.4 Tipps und Tricks

QEMU besitzt einen eigenen DHCP-Server und vergibt die IP-Adresse 10.0.2.15 an das virtuelle Puppy-Linux. Die Netzwerkkarte konfigurieren Sie mit dem Wizard „Menu - Setup - Network Wizard“. Vom Host-System können Sie die virtuelle Instanz nicht erreichen. Dies verhindert QEMU. In die andere Richtung funktioniert es allerdings. Sie können sowohl ins Internet als auch auf das native Host-System zugreifen.

Eine weitere Besonderheit von QEMU-Puppy ist, dass Sie es auch ohne Host-System direkt von einem USB-Stick starten können. Dazu müssen Sie allerdings zunächst den USB-Stick bootfähig machen. Unter Linux geschieht dies mit dem Befehl `syslinux /dev/<usbgerät>` und `<Laufwerksbuchstabe>:\syslinux <Laufwerksbuchstabe>` unter Windows. Dann haben Sie das Betriebssystem als Live-Version nativ auf dem Host-Rechner laufen.

Verbunden: Von der virtuellen Instanz ist es kein Problem ins Internet zu kommen.

Allerdings gibt es hier manchmal Probleme mit USB-Geräten, die größer als ein GByte sind. Speziell dann, wenn die Cluster-Größe 16KByte übersteigt. Das trifft üblicherweise auf Massenspeicher mit mehr als einem GByte zu. Schuld hierfür ist der Boot-Loader SysLinux (http://syslinux.zytor.com).



So funktioniert es: Diese Grafik zeigt, welche Verwendung die einzelnen Dateien haben und deren Mount-Punkte. (Quelle: http://erikveen.dds.nl)

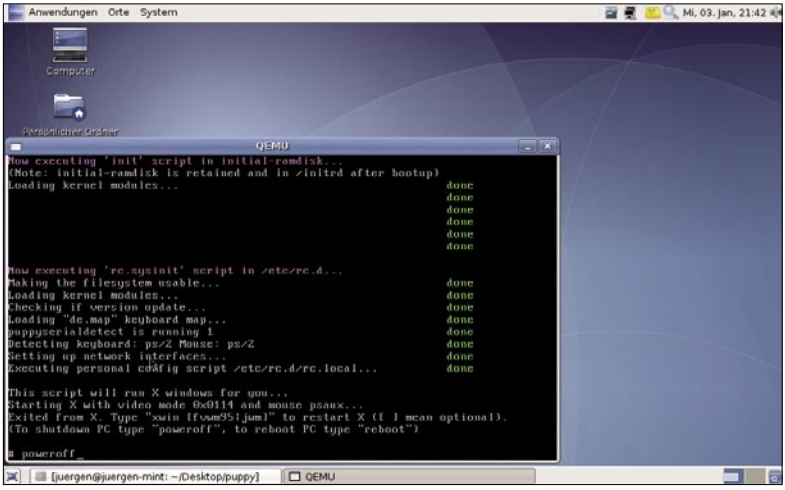
Interessante Dateien

In der Datei *pup_save.3fs* sind alle Benutzerdaten gespeichert, also Ihre persönlichen Einstellungen und neu angelegten Dateien. Um auf diese Daten Einsicht zu haben, müssen Sie nicht zwingend QEMU-Puppy starten. Diese Datei lässt sich als Loopback-Gerät in jedes andere Linux-Betriebssystem einbinden:

Die Datei *ext_212.sfs* ersetzte der Entwickler durch eine leere Version. Laut eigener Aussage wollte er damit Platz sparen. Normale Anwender brauchen diese Datei nicht wirklich. Das Original benötigen Sie lediglich, wenn Sie eigens Programme kompilieren möchten. Sie können eine original *ext_212.sfs* von der Puppy-Seite www.puppyos.com herunterladen und diese verwenden. Es muss sich jedoch immer eine dieser Dateien auf dem USB-Stick befinden. Andernfalls würde QEMU-Puppy nicht starten. Es lohnt sich auch ein Blick auf die Projekt-Seite www.erikveen.dds.nl/qemupuppy/index.html#6.3.0. Dort finden Sie zum Beispiel ein Script, wie Sie mehrere Klons einer QEMU-Puppy-Instanz auf der selben Maschine laufen lassen können. Laut Entwickler kostet jeder Klon nur 172 KByte zusätzlichen Speicherplatz. Das ist selbstverständlich ohne Anwender-Daten.

Herunterfahren von QEMU-Puppy

Der Test hat gezeigt, dass Veränderungen im System ausschließlich dann gespeichert werden, wenn Sie das Betriebssystem sauber herunterfahren. Hier erlebt man eine kleine Überraschung. Denn die Schaltflächen „Reboot Computer“ und „Power-off Computer“ führen lediglich zu einem Neustart des X-Servers. Es ist aber mit einem kleinen Umweg trotzdem möglich.



Doppelschritt: Wenn Sie zunächst den X-Server herunterfahren ist ein Herunterfahren des virtuellen Systems möglich.

Der Trick ist, dem Betriebssystem zunächst mit „Exit to prompt“ den X-Server zu entziehen. Danach haben Sie die Möglichkeit mit „poweroff <enter>“ das virtuelle System herunterzufahren. Ähnlich verhält es sich mit dem Befehl „reboot“, der QEMU-Puppy neu startet.

Dateien transferieren

Laut Entwickler ist der Transfer von Dateien von der virtuellen Maschine zum Host-System nicht ganz trivial. Als besten Weg schlägt er eine Kombination aus *tar* und *nc* vor. Linux stellt diese Software normalerweise von Haus aus bereit. Für Windows stellt er tar.exe (http://www.erikveen.dds.nl/qemupuppy/diverse/tar.exe) und nc.exe (http://www.erikveen.dds.nl/qemupuppy/diverse/nc.exe) als Download zur Verfügung. Ein Upload zu QEMU-Puppy sähe zum Beispiel so aus: `tar cv <Dateien> | nc -l -p 1234 -w 10`. Eine genaue Anleitung finden Interessierte Sie auf der Projekt-Seite. Es ist ebenfalls möglich, Daten mittels Samba zu transferieren. Dazu müssten Sie ihr QEMU-Puppy anpassen. In der Datei */etc/rc.d/rc.local* könnten Sie folgende Einträge hinzufügen:

```
mkdir /<Verzeichnis>
smbmount //<SMB-Server>/qemu /<Verzeichnis> -o guest
```

Das Verzeichnis <Verzeichnis> wäre beim Aufruf des Startscripts mit der Option -smb /<Verzeichnis> verbunden: `./puppy.sh –smb /<Verzeichnis>`

2.1.5 Fazit

QEMU-Puppy ist ein sehr interessanter Ansatz für ein schlankes Betriebssystem zum Mitnehmen. Es bringt viele nützliche, schlanke Applikationen mit, die man für unterwegs benötigt. Ein denkbarer Einsatz ist zum Beispiel auf Reisen. Wenn man sich die Rechner in einigen Internet-Cafes ansieht, kommt einem das blanke Grauen. Verseucht mit Spyware und Viren tippt man ungern irgendein Passwort in so ein System. Mit QEMU-Puppy gehört dies der Geschichte an.

An einigen Stellen hakt es noch und es bedarf Verbesserungen. Fairerweise muss man sagen, dass QEMU nicht die schnellste Virtualisierungs-Lösung ist. Aber mit einer Bildschirm-Auflösung von 800x600 und 16bit Farbtiefe lässt sich damit ganz gut arbeiten. Bei den heutigen USB-Stick-Größen tut es jedenfalls nicht weh, ein Betriebssystem vom Format QEMU-Puppy für den Notfall dabei zu haben.

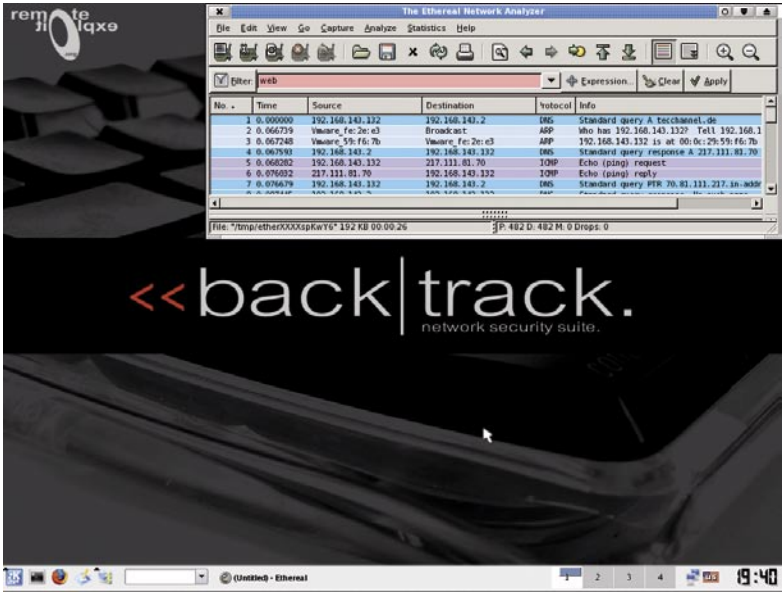
Jürgen Donauer

tecCHANNEL-Links zum Thema	Webcode	Compact
QEMU-Puppy-Linux: Virtualisierung in der Hosentasche	458934	S.75
17 Linux Distributionen für den Spezialeinsatz	455960	S.83
32 Linux Distributionen für den Client-Einsatz	454188	–

2.2 17 Linux-Distributionen für den Spezialeinsatz

In die Kategorie „Spezialeinsatz“ fallen beispielsweise solche Distributionen, die sich einem ganz bestimmten Einsatzzweck wie beispielsweise als Router oder als Mediaplayer. Mini-Distributionen eignen sich hervorragend für ältere Hardware oder als Betriebssystem auf einem USB-Stick – etwa wenn man dem installierten OS nicht traut oder besondere Funktionen wie Datenrettung oder Partitionierung im mobilen Support-Einsatz benötigt.

Linux stellt allerhand Werkzeuge zur Verfügung. Dazu gehören auch so genannte Sniffer und Tools zum Knacken von Passwörtern oder WLAN-Schlüsseln. Um Schwachstellen in ihren Systemumgebungen aufzuspüren sind diese Tools ein Segen. Oftmals ist man sich gar nicht bewusst, welche Schluchten sich in einem Security-Konzept befinden. Nur wer weiß, wie Hacker arbeiten, kann sich vor Angriffen schützen. Diese Programme lassen sich allerdings auch nutzen, um sich in illegales Terrain zu begeben. tecCHANNEL möchte Sie ausdrücklich warnen, dass Sie sich mit einer Benutzung solcher Programme strafbar machen können. Wollen Sie so eine Distribution im Firmen-Netzwerk einsetzen, stellen Sie sicher, dass diese Maßnahme abgesegnet ist.



Sicherheit im Umfeld: Mit BackTrack können Sie Schwachstellen aufspüren und entsprechende Gegenmaßnahmen ergreifen.

2.2.1 BackTrack

BackTrack (www.remote-exploit.org) ist eine Live-CD und ein Zusammenschluss der wohl bekanntesten Sicherheits-Distributionen Whax und Auditor. Die Entwickler legten die beiden Distributionen zusammen und kreierten ein „Best of both worlds“. Das Ergebnis kann sich sehen lassen.

Diese Distribution lässt keine Wünsche offen, wenn es um das Aufspüren von Sicherheitslöchern geht. Auf der Webseite befindet sich eine Untersektion mit Tutorials. Dort wird ihnen gezeigt, wie Sie die auf der CD befindlichen Tools optimal einsetzen. Der eine oder andere dürfte beim Zusehen der Flash-Demonstrationen große Augen machen. Es ist erstaunlich, wie einfach sich zum Beispiel WEP-Schlüssel knacken oder andere Schwachstellen ausnutzen lassen.

2.2.2 Damn Small Linux und Damn Small Linux Not

Damn Small Linux (www.damnsmalllinux.org) ist eine extrem kleine Linux-Distribution. Die Entwickler haben es sich zur Aufgabe gemacht, die Grenze von 50 MByte nie zu überschreiten. Dennoch wollen Sie eine vollständige Desktop-Umgebung zur Verfügung stellen. Das beinhaltet zum Beispiel XMMS, Xpdf, einen Chat-Client, einen Internet-Browser, einen E-Mail-Client, ein Textverarbeitungs- und Tabellenkalkulations-Programm.

Verdammt klein: Damn Small Linux ist klein aber oho!

Der Lightweight Desktop-Manager Fluxbox dient zur graphischen Darstellung. Mittlerweile basiert DSL auf Knoppix-Technologie. Damn Small Linux bootet sich, wenn möglich, komplett in den RAM eines Systems und ist dadurch sehr schnell. Sie können DSL ebenfalls auf Festplatte installieren. Somit wird es zu einem Debian-System und Sie haben Zugriff auf die kompletten Debian-Repositories. Damn Small Linux lässt sich übrigens auch auf einen USB-Stick installieren. Weiterhin können Sie ein Image herunterladen, das Sie danke qemu direkt in Windows starten können.

Damn Small Linux Not (www.damnsmalllinux.org/dsl-n/) ist von denselben Leuten gemacht. Dieses System hat allerdings nicht den Anspruch der 50-MByte-Grenze. Dennoch wollen die Entwickler unter allen Umständen so genannte „Bloatware“ vermeiden. Dieser Fork von DSL war eine logische Konsequenz des immer größer werdenden Linux-Kernels. DSL setzt noch auf Kernel 2.4 wogegen DSL-N den moderneren Kernel 2.6 zum Einsatz bringt. Was sich nicht mehr in 50 MByte unterbringen lässt, aber trotzdem wertvolle Tools sind, packen die Entwickler in DSL-N. Dazu gehören unter anderem Samba und LinNeighbourhood. Ebenso sind die Madwifi-Treiber und fuse/sshfs enthalten.

2.2.3 Feather Linux

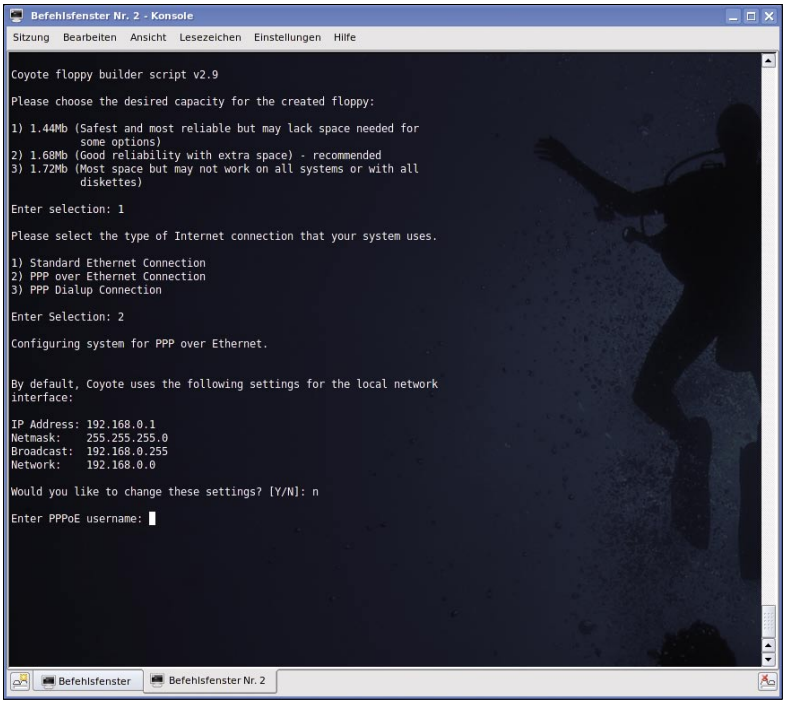
Feather Linux (http://featherlinux.berlios.de) ist ein Remaster von Knoppix, läuft komplett von CD oder USB-Gerät und braucht weniger als 128 MByte Speicher. Dennoch ist es reich mit Software bestückt.

Federleicht: Feather Linux überzeugt durch Geschwindigkeit und Paketauswahl.

Es sollte den Großteil abdecken, was man für die tägliche Arbeit benötigt. Darunter befinden sich zum Beispiel Abiword, Firefox, Capticve-NTFS, gaim, vim, Sylpheed, XMMS, FreeNX, Midnight Commander, Samba und viele andere. Das System ist klein und extrem schnell. Feather Linux ist nicht sehr hardwarehungrig und kann ältere Systeme zu neuen Höhen verhelfen.

2.2.4 Fli4l und Coyote Linux

Fli4l (www.fli4l.de) steht eigentlich für „floppy isdn4linux“. Dieser Titel ist allerdings alles andere als zeitgemäß. In der Zwischenzeit kann fli4l nämlich auch mit DSL und Ethernet-Routing umgehen. Außerdem ist das Betriebssystem mittlerweile als CD erhältlich. Das Projekt stellt weiterhin Treiber für AVM- und Atheros-Hardware zur Verfügung. Mit letzteren können Sie einen Access-Point mit optionaler WPA2-Verschlüsselung realisieren.

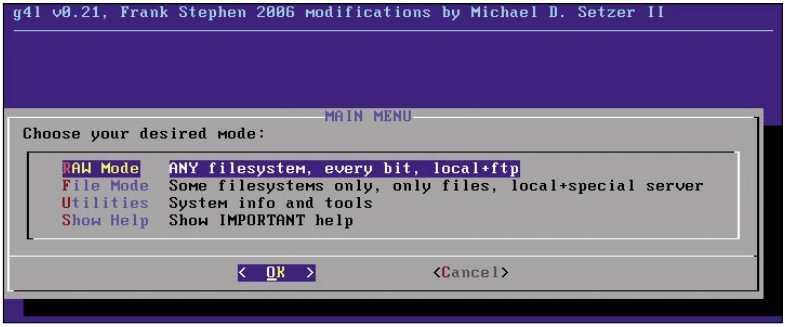


Unscheinbarer Zauberer: Der Weg zum Ziel muss nicht immer mittels grafischen Wizards erfolgen und kann trotzdem einfach sein.

Coyote Linux (www.coyotelinux.com) war ursprünglich als Floppy-Router-System gedacht. So können Sie einen Uralt-PC ohne Festplatte und CD-Laufwerk als Internet-Sharing-Maschine nutzen. Dieses Projekt existiert immer noch. Mittlerweile hat sich die Produkt-Palette aber erweitert. So bietet die Firma „Wolverine Firewall and VPN-Server“ und sogar fertige Hardware-Appliances an. Damit hat sich im Laufe der Jahre die Zielgruppe von Coyote Linux vom Privatanwender über Small-Offices bis hin zu großen Firmen kontinuierlich erweitert.

2.2.5 G4L (Ghost for Linux)

G4L (http://sourceforge.net/projects/g4l) erhebt den Anspruch, ein Ghost-Klon mit freier Software zu sein. Das gelingt der Distribution auch ganz gut. Allerdings ist die Handhabung auf den ersten Blick nicht ganz so trivial wie das berühmte Vorbild Norton Ghost. Hat man sich aber erst einmal zurecht gefunden, bietet dieses OS alles Notwendige, um Abbildungen von Partitionen oder ganzen Festplatten zu generieren. G4L bietet keine Klicki-Oberfläche. Dennoch ist die graphische Benutzerführung erträglich. Sie können dank eine RAW-Modus jedes Datei-System klonen. Dazu gehören auch Windows-Partitionen.



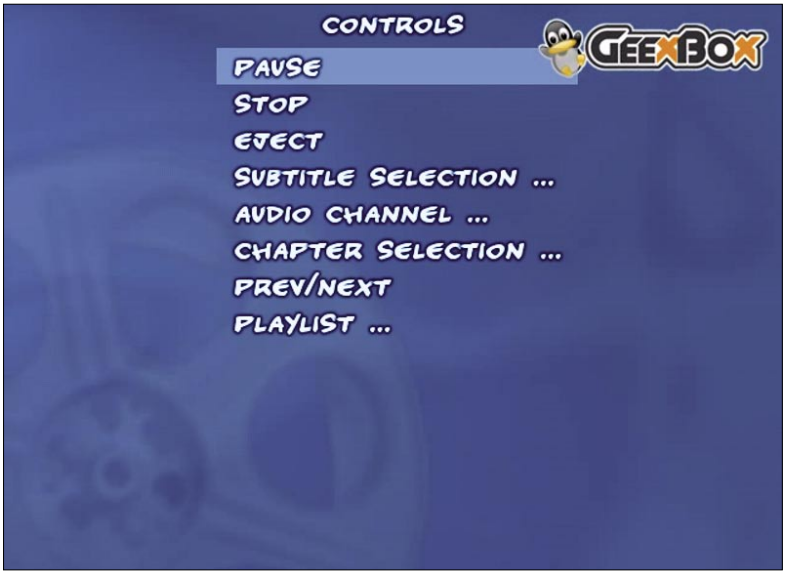
Die Geister, die ich rief: Versteht man erst das Prinzip von G4L, ist das Klonen ein Kinderspiel.

Die kreierten Images können Sie auf Verlangen komprimieren. Außerdem ist nicht nur ein lokales Klonen möglich, sondern auch via FTP auf Netzlaufwerke. Weitere Goodies, wie zum Beispiel das Partitionierungs-Werkzeug parted befinden sich ebenfalls auf dem ISO-Image.

2.2.6 GeeXboX

GeeXboX (www.geexbox.org) ist eine komplette Linux-Distribution. Mit der Ausnahme, dass dieses Betriebssystem auf dem Multimedia-Tausendsassa MPlayer basiert. Sie müssen das System nicht auf Festplatte installieren, sondern können es

komplett von CD laufen lassen. GeeXboX bietet eine simple Oberfläche und verwandelt Ihr System in eine Multimedia-Station. Sie können damit nahezu jedes Datei-Format abspielen. Mittlerweile unterstützt das OS auch DVDs und die Navigation durch deren Menus. Ebenso unterstützt GeeXboX Shoutcast und Netstream. Auch diverse TV-Karten stehen auf der Support-Liste des Betriebssystems.

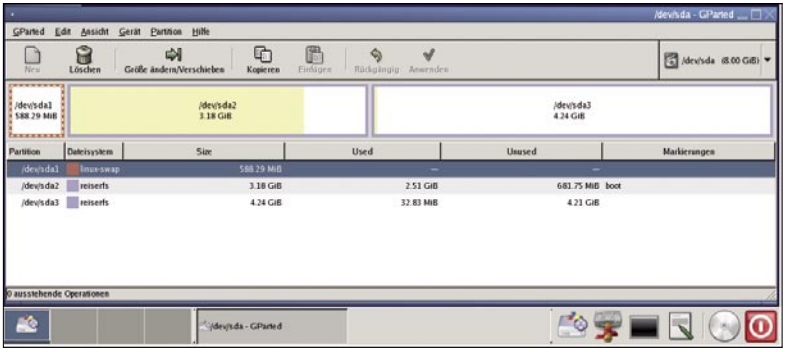


Multimedia: GeeXboX verwandelt Rechner der Pentium-Klasse in eine Multimedia-Station um.

Ein auf der Seite bereit gestellter ISO-Generator erlaubt es Ihnen, das Image neu zu gestalten. Damit können Sie zum Beispiel unfreie Codecs oder extra Themes hinzufügen. Ebenso lassen sich damit Startverhalten von MPlayer, Netzwerkeinstellungen und diverse andere Parameter einstellen. Beeindruckend ist außerdem die Größe des ISO-Image von GeeXboX: 6,8 MByte.

2.2.7 GParted Livecd

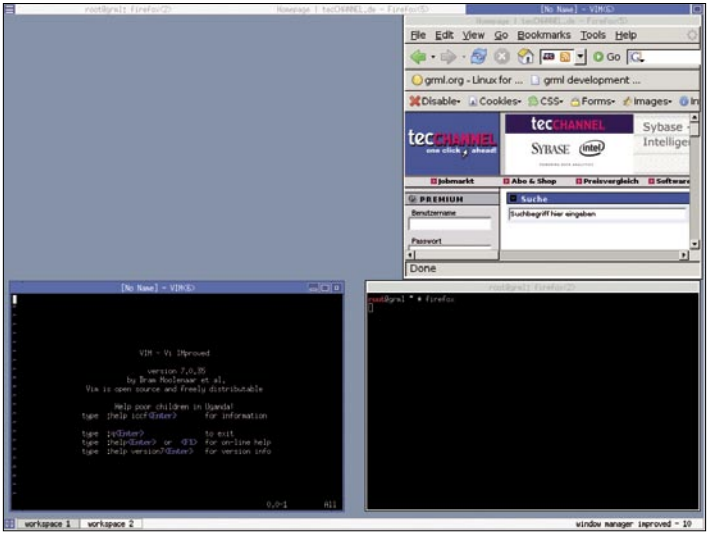
GParted Livecd (http://gparted.sourceforge.net) wurde eigentlich zu einem einzigen Zweck geschaffen. Es soll als mobiles Partitionierungs-Tool dienen. Die Distribution bootet nach Auswahl von Sprache und Tastaturbelegung in eine grafische Umgebung. Hierfür verwendet sie Fluxbox. Außer dem Partitionierungs-Tool sind noch ein simpler Texteditor und eine Terminal-Emulation enthalten. Doch seinem Anspruch, ein simples Partitionierungs-Tool zu sein, wird die Distribution vollkommen gerecht.



Mobil Partitionieren: GParted Livecd macht das Umpartitionieren einer oder mehrerer Festplatten zu einem Kinderspiel.

2.2.8 grml

grml (www.grml.org) basiert auf Knoppix und richtet sich speziell an System-Administratoren oder Liebhaber von Text-Tools. Es ist geeignet als Rescue-System, für die Netzwerk-Analyse oder für Hartgesottene als Desktop-Umgebung. Programme wie KDE und OpenOffice sucht man vergebens auf der Live-CD. Dafür enthält es über 800 Pakete, die Sie bei Knoppix nicht finden.

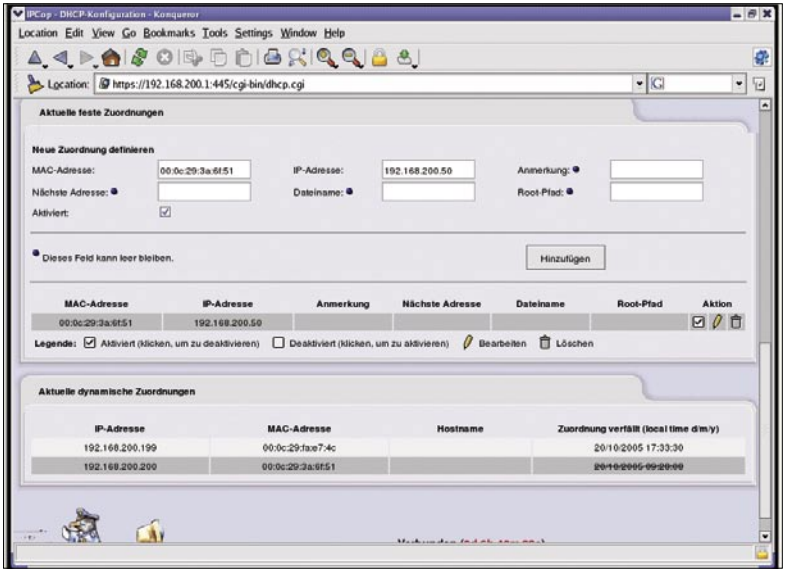


Nichts für Klickibuntis: grml bietet fast alles für Text-Tool-Fans. Aber auch grafische Anwendungen enthält die Distribution.

Dank Zugriff auf die umfangreichen Debian-Repositories können Sie jedoch aus der Distribution machen, wie ihnen der Gusto steht. Eine Sache ist jedenfalls unbestritten: Gäbe es einen „Funny Codename Soundalike Contest“, wäre grml der ungekrönte König. Arbeitsnamen wie Winterschlapfn, Bootenschnitzl, Funkenzutzler und Eierspass sind wohl kaum zu toppen.

2.2.9 IPCop Firewall

IPCop Firewall (www.ipcop.org) ist eine komplette Linux-Distribution, die sich um das Heil ihres Netzwerks kümmern möchte. Wahlspruch der Entwickler ist: „The bad packets stopp here!“. Das heißt IPCop bietet eine komplette kostenfreie Firewall mit Gateway-Funktionen. Daneben bietet die Distribution unter anderem einen DHCP- und Proxy-Server, so wie ein VPN-Gateway. Intrusion-Detection steht ebenfalls auf dem Programm des IP-Polizisten. Nach einer erfolgreichen Installation administrieren Sie das Komplett-Paket bequem über ein Web-Frontend. Sie müssen also kein Linux-Freak sein um diese Firewall unter Kontrolle zu halten. Wie Sie IPCop perfekt einsetzen, zeigt ihnen der tecCHANNEL-Online-Artikel „IPCop – Die Profi-Linux-Firewall-Distribution“ (**Webcode 433444**).

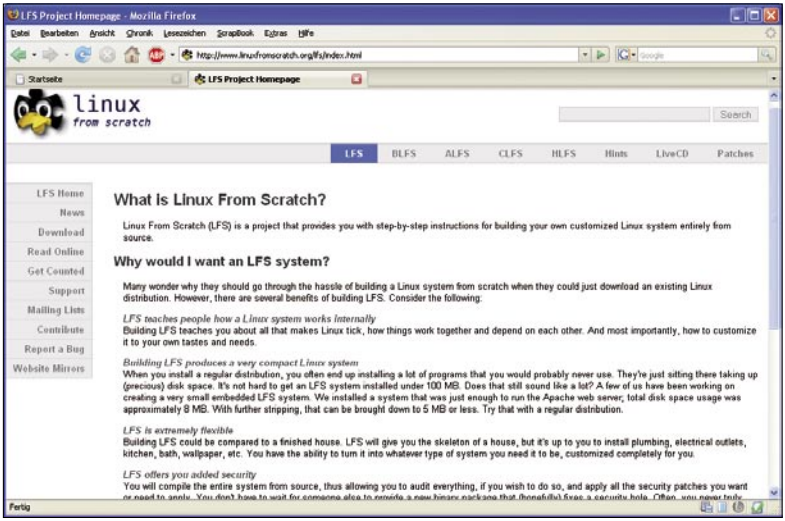


Nicht nur eine Firewall: IPCop dient unter anderem auch als DHCP-Server.

2.2.10 Linux From Scratch

Linux From Scratch (www.linuxfromscratch.org) ist ein Projekt, dass es Ihnen erlaubt ein komplettes Linux-System von Grund auf zu erstellen. Die lauteste Credo in Zusammenhang mit dieser Distribution dürfte sein: „Warum soll ich es mir antun, ein System von Grund auf selbst zu kompilieren? Es ist doch viel einfacher eine existierende Distribution wie Mandriva oder Fedora Core zu installieren.“.

LFS richtet sich nicht an Anfänger. Aber es kann Leuten zeigen, wie Linux intern arbeitet. Ein eigenes System von der Basis zu basteln zeigt ihnen, wie Dinge zusammen arbeiten und von einander abhängig sind. Logischerweise können Sie auch ein System erstellen, dass genau ihren Ansprüchen genügt. Linux From Scratch ist nicht trivial. Es gibt jedoch zahlreiche Dokumentationen, die ihnen behilflich sind. Die deutsche Übersetzung der Doku finden Sie hier. Allerdings sollten Sie einiges an Zeit reservieren, wenn Sie diese Mission angehen wollen.



Braucht Zeit: Mit Linux From Scratch lassen sich maßgeschneiderte Systeme erstellen.

2.2.11 Linux LiveCD Router

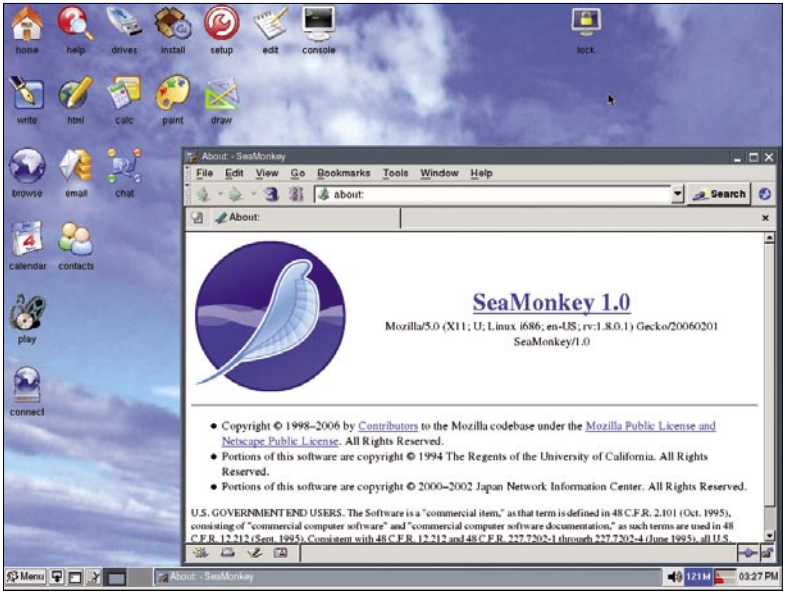
Linux LiveCD Router (www.easylivecd.com/english/cdrouter.html) ist speziell für das Sharing einer Internet-Verbindung via WiFi erschaffen. Die Installation auf Festplatte ist nicht notwendig und auch gar nicht möglich. Sie können das OS mit DSL,- Kabel-Modem-, T1-, ISDN- oder Dial-Up-Verbindungen nutzen. Bei Bedarf dient diese Variante auch als Firewall oder sogar als Access-Point für Wireless-Lan-Karten.

```
Linux LiveCD Router V 2.0.14  EasyLiveCD.com

Features:

 Share and Firewall your broadband
 Does not require installation
 Traffic control and QoS
 Remote SSH administration
 Remote secure access and browsing
 Can save configuration to floppy
 Supports Broadband, Cablemodem, DSL, WiFi
 Frame Relay, Dial-Up, WiFi

 Note:  You can not eject the cdrom while using the LiveCD Router
        To finish reboot using Ctrl+Alt+Delete

        To login initially use login: root  pass: cdrouter
```

Kostenloser Router und Accesspoint: Denkbar für den Einsatz des Linux LiveCD Router ist längst veraltete Hardware.

2.2.12 Puppy Linux

Puppy Linux (www.puppylinux.org) ist eine weitere extrem kleine Distribution. Hat ein Rechner mindestens 128 MByte RAM zur Verfügung, lädt sich das Betriebssystem komplett in den Arbeitsspeicher.



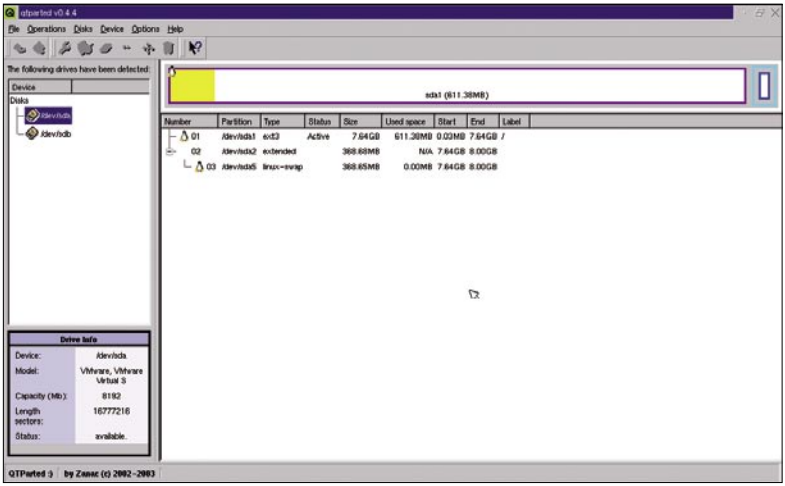
Alles an Bord: Es ist schon beeindruckend, welch Vielzahl an Software man auf unter 100 MByte pressen kann.

Somit läuft das Laden von Applikationen in Puppy Linux unglaublich schnell ab. Die Hardware-Anforderungen des OS sind gering. Ein Einsatz auf älterer Hardware ist somit kein Problem. Sie können das OS auf Festplatte oder ein USB-Gerät installieren. Obwohl das ISO-Image derzeit unter 100 MByte hat, finden Sie darauf eigentlich alles, was Sie zur täglichen Arbeit brauchen.

Eine echte Besonderheit von Puppy Linux ist, dass Sie alle Veränderungen direkt wieder auf CD zurück schreiben können. Die unkomplizierte Menu-Führung macht Puppy Linux auch für Einsteiger interessant.

2.2.13 SystemRescueCD

SystemRescueCD (http://sysresccd.org) gehört definitiv zur Kategorie „Admins Best Friend“. Wie der Name der Distribution vermuten lässt, wurde die Live-CD für den „Worst Case“ entwickelt. Die Distribution soll ihnen nach dem Crash helfen. Das OS enthält unter anderem die Partitionierungs-Werkzeuge QtParted und PartGui. Weiterhin finden Sie den Drive-Image-Klon Partimage auf der CD. Antiviren-Scanner, Rootkit-Detektion, Archivierungs-Tools, Brennprogramme und Netzwerk-Programme lässt SystemRescueCD ebenfalls nicht missen.



Admins Best Friend: Nach dem Crash ist vor SystemRescueCD.

Um Windows-Laufwerke lesen und beschreiben zu können dient Captive NTFS. Trotz umfangreicher Software ist das Betriebssystem klein genug für eine Business-Card-CD. Die meisten Tools können sie zwar nur auf Kommandozeilen-Eben nutzen, dennoch lohnt sich ein Blick auf diese Distribution.

Linux-Distributionen im Überblick

Anbieter	Produkt	Internet	Einsatz	Varianten	
BackTrack	BackTrack 1.0	www.remote-exploit.org	Security, Desktop	BackTrack	
Damn Small Linux	Damn Small Linux 3.0	www.damnsmalllinux.org	Desktop	Damn Small Linux	
Damn Small Linux	Damn Small Linux Not 0.1-RC4	www.damnsmalllinux.org	Desktop	Damn Small Linux Not	
Feather Linux	Feather Linux 0.7.5	featherlinux.berlios.de	Desktop	Feather Linux	
Fli4l	Fli4l 3.0	www.fli4l.de	Firewall, Router	Floppy-, CD-Version	
G4L	G4L 0.21	sourceforge.net/projects/g4l	System-Tools	G4L	
GeeXbox	GeeXbox 1.0	www.geexbox.org	Desktop	GeeXboX	
Gparted	Gparted Livecd 0.2.5-5	gparted.sourceforge.net	System-Tools	Gparted Livecd	
grml	grml 0.8	www.grml.org	Desktop	grml	
IPCop	IPCop Firewall 1.4.11	www.ipcop.org	Firewall, VPN-Server	IPCop	
Linux From Scratch	Linux From Scratch 6.2	www.linuxfromscratch.org	Desktop, Server	Linux From Scratch	
Musix GNU+Linux	Musix GNU+Linux 0.49	www.musix.org.ar	Desktop	Musix GNU+Linux	
Puppy Linux	Puppy Linux 2.02	www.puppylinux.org	Desktop	Puppy Linux	
System RescueCD	System RescueCD 0.2.19	sysresccd.org	System-Tools	System RescueCD	
VideoLinux	VideoLinux	www.videolinux.net	Desktop	VideoLinux	
Vortech	Coyote Linux 3.00.46	www.coyotelinux.com	Firewall, Router	Floppy-, Festplatten-Version	
WiFi.com.ar	Linux LiveCD Router	www.easylivecd.com/english/cdrouter.html	System-Tools	Linux LiveCD Router	

	Architektur	Besonderheit	Kernel / glibc	X-Server / GUI	Preis
	i486	große Sammlung an Sicherheits-Tools, gute Anleitungen auf der Webseite	2.6.15.6 / 2.3.5	X.org 6.9.0 / KDE 3.5.0	frei
	i386	nur 50 Mbyte groß, seh schnell	2.4.26 / 2.3.2	Xfree86 4.3.0 / Fluxbox 0.1.14	frei
	i386	klein, schnell, moderner Kernel	2.6.12 / k. A.	k. A. / k. A.	frei
	i386	klein, schnell	2.4.27 / 2.3.2	Xfree86 4.3.0 / Fluxbox 0.9.10	frei
	k. A.	PC in einen Router verwandeln	k. A. / k. A.	keine / keine	frei
	k. A.	Ghot-/DriveImage-Klon	k. A. / k. A.	k. A. / k. A.	frei
	i386, ppc	Verwandelt PC in Multimedia-System	k. A. / k. A.	k. A. / k. A.	frei
	i486	Partition-Magic-Klon	2.6.17.7 / 2.3.4	X.org 6.8.2 / Fluxbox 1.0rc2	frei
	i486	viele Shell-Tools, gut für Systemadministratoren	2.6.17.7 / 2.3.6	X.org 7.0 / WMI	frei
	i386, alpha	einfach per Web-GUI zu administrieren	2.4.31 / 2.3.3	keine / keine	frei
	i386	Linux von grund auf selbst kompilieren	2.6.16.27 / 2.3.6	keine / keine	frei
	i486	umfangreiche Sammlung an Audio-Werkzeugen	2.6.16 / 2.3.6	X.org 6.9.0 / KDE 3.5.1	frei
	i386	klein, schnell, moderner Kernel, kann Veränderungen direkt auf CD zurückschreiben	2.6.16.7 / 2.3.4	X.org 6.8.1	frei
	i386	Rettungs-CD nach einem System-Crash	2.6.16.10 / 2.3.2	keine / keine	frei
	i586	umfangreiche Sammlung an Multimedia-Werkzeugen	k. A. / k. A.	X.org 6.9.0 / KDE 3.5.1	frei
	i486	PC in einen Router verwandeln	k. A. / k. A.	keine / keine	frei
	k. A.	Internet-Sharing	k. A. / k. A.	k. A. / k. A.	frei

2.2.14 VideoLinux und Musix GNU+Linux

VideoLinux (www.videolinux.net) basiert auf PCLinuxOS und legt das Hauptaugenmerk auf den Multimedia-Bereich. Es befinden sich darin Tools für DVD-Backups, Video Encoding und Trancoding, DVD-Author-Werzeuge, Format-Konvertierung und viele andere. Die Entwickler schreiben sich „The all in one Toolkit for DVD Ripping, Encoding & Editing“ auf die Fahnen und den Bootscreen. Sie finden nicht alltägliche Tools, wie zum Beispiel DeVeDe, VirtualDub (WINE), DVDShrink, LiVEs und Avidemux auf dieser Distribution. Interessant an dieser Version ist die Tatsache, dass es mehr hervorragende Multimedia-Tools für Linux gibt, als so manch einer glauben mag.

Multimedia-Studio: VideoLinux bietet ihnen eine vollständige Plattform, um Multimedia-Dateien zu bearbeiten.

Musix GNU+Linux (www.musix.org.ar) ist Knoppix-basierend und hat sich auf frei erhältliche Audio-Software spezialisiert. Es richtet sich in erster Linie an Musik-Liebhaber, Musiker und DJs. In dieser Linux Variante finden Sie zum Beispiel HEXTER. Das ist ein „Yamaha DX-7 Software Synthesizer“. Weiterhin befinden sich unter anderem der MIDI-Sequencer Rosegarden und der Percussion-Emulator Hydrogen an Bord. Es existiert unter der Adresse http://lam.fugal.net sogar eine Seite mit Musikstücken, die mit dieser Distribution erstellt wurden.

2.2.15 Fazit

Es gibt für fast jedes Anwendungsgebiet eine Linux-Distribution, die genau dessen Ansprüche erfüllt. Vor allem im Sicherheitsbereich tummeln sich einige sehr interessante Varianten. Mini-Distributionen wie zum Beispiel Damn Small Linux und Puppy Linux sind in zweierlei Hinsicht hochinteressant. Da diese sehr wenig System-Resourcen brauchen eignen sich diese hervorragend als portable Client-Systeme. Zum zweiten hauchen Sie damit alten Rechnern neues Leben mit aktueller Software ein.

Spezielle Betriebssysteme wie zum Beispiel Gparted Linux und G4L sollen ihnen bestimmte Arbeiten erleichtern. Diese booten oft schnell und haben nur wenige Applikationen an Bord. Dennoch sind diese kostenlosen Helferlein oft ein wahrer Segen in der täglichen Arbeit. Man sollte auch BackTrack zu diesen Distributionen zählen. Erschaffen ist das OS, um die Sicherheit zu erhöhen. Dennoch könnten Sie damit viel Unfug treiben. tecChannel möchte Sie deswegen noch einmal darauf hinweisen, dass Sie sich mit den darin bereit gestellten Tools schnell am Rande der Legalität bewegen.

Mike Hartmann, Jürgen Donauer

tecCHANNEL-Links zum Thema	Webcode	Compact
17 Linux-Distributionen für den Spezialeinsatz	455960	S.
32 Linux-Distributionen für den Client-Einsatz	454188	–
25 Linux-Distributionen für den Server-Einsatz	447420	–
IPCop – Die Profi-Linux-Firewall-Distribution	433444	–

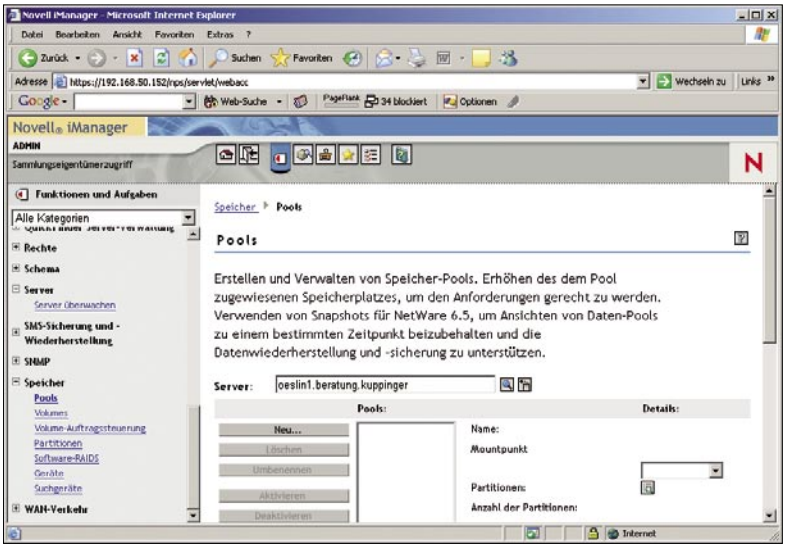
Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

2.3 Novells Dateisystem unter Linux

Mit dem OES (Open Enterprise Server) hat Novell im Jahr 2005 eine Plattform vorgestellt, die Linux und NetWare miteinander verbindet. Basierend auf einem NetWare- oder Linux-Kernel können die wichtigsten NetWare-Dienste genutzt werden. Das eDirectory, die File- und Printserver-Dienste und die Cluster-Dienste stehen auf beiden Plattformen zur Verfügung. Die Integration geht so weit, dass sogar gemischte Cluster mit Knoten, die teils unter NetWare und teils unter Linux arbeiten, realisiert werden können.

Da die Fileserver-Funktionalität immer eine Stärke der NetWare war, ist dieser Dienst im Zusammenhang mit dem OES besonders interessant. Es gibt unter Linux zwar etliche Dateisysteme wie Ext2 (Second Extended File System), Ext3 (Third Extended File System), ReiserFS (Reiser File System), JFS (Journaling File System) oder XFS (Extended File System).

Die Novell Storage Services (NSS) machen trotz der großen Auswahl Sinn. Die enge Integration mit dem Novell eDirectory, die sehr differenzierten Zugriffsberechtigungen, eine einfache Konfiguration über Pools und der Fakt, dass es das Dateisystem ist, das als einziges in gemischten Clustern des OES genutzt werden kann, stellen die wichtigsten Gründe für seine Nutzung dar.

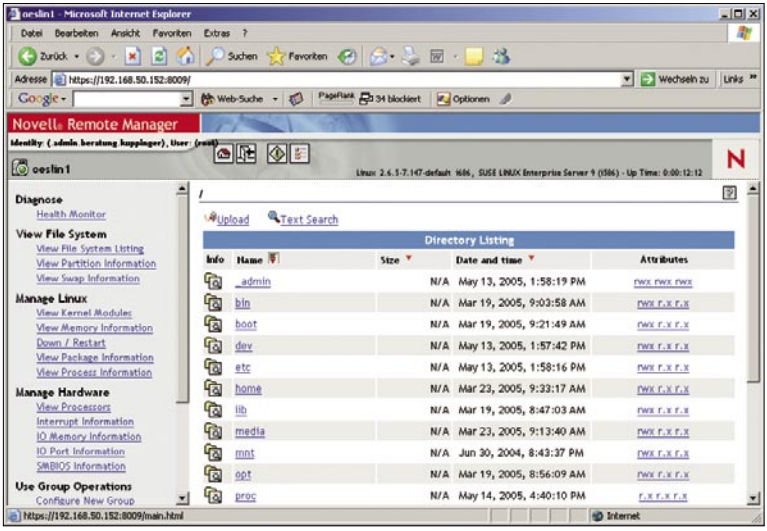


Einfach: Die Funktionen für das Management von Pools und Volumes stehen sowohl unter NetWare als auch Linux zur Verfügung und bieten eine hohe Flexibilität bei der Konfiguration der NSS.

Es gibt zwar einige kleinere Unterschiede zwischen der NetWare- und der Linux-Variante. So werden die Archivierungs- und Versionierungsdienste unter Linux bisher nicht unterstützt. Außerdem können Verschlüsselungsfunktionen in gemischten Clustern nicht eingesetzt werden. Insgesamt ist die Kompatibilität aber doch sehr hoch. Und für den isolierten Betrieb nur auf dem OES for Linux spielen die meisten Unterschiede ohnehin keine Rolle.

2.3.1 Wichtige Details zu den NSS und die Rolle von NCP

Die NSS für Linux unterscheiden sich in einigen wichtigen Details von der NetWare-Version, sowohl in Bezug auf die Implementierung als auch die Administration. So unterstützt beispielsweise der Novell Remote Manager (NRM) in der Linux-Variante im Gegensatz zu NetWare-Servern kein Partitionsmanagement. Das ist aber insofern kein Problem, als der iManager für das Pool- und Volume-Management sowohl bei Linux- als auch NetWare-Plattformen eingesetzt werden kann und das grundlegende Partitionsmanagement mit YaST erfolgt.



Nicht vollständig: Beim Novell Remote Manager für die Linux-Version des OES fehlt die Funktionalität für das Partitionsmanagement der NSS, so dass hier mit dem iManager respektive mit lokalen Tools unter Linux gearbeitet werden muss.

Auf der technischen Ebene gibt es bei den so genannten Security Equivalence Vectors (SEVs) Unterschiede. Die SEVs beschreiben die Sicherheitsinformationen für Benutzer. Bei NetWare werden diese beim Verbindungsaufbau eines Be-

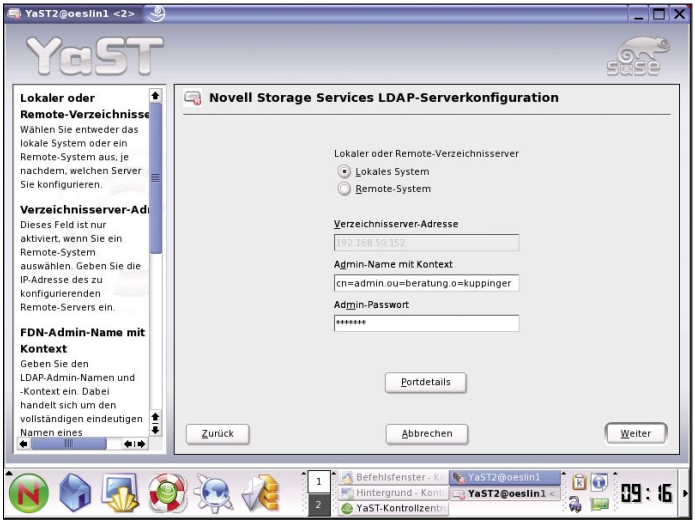
nutzers zu den NSS vom eDirectory angefordert und anschließend als Teil der Verbindung verwaltet. Die Lebensdauer des SEVs bei der Nutzung der NSS entspricht damit der Lebensdauer der Verbindung.

Bei Linux-Servern mit dem OES werden die Informationen dagegen beim ersten Zugriff in den Cache genommen und verbleiben dort bis zum Neustart eines Servers oder dem Löschen des Benutzers aus dem eDirectory. Sie werden aber regelmäßig aktualisiert, wobei das Aktualisierungsintervall konfigurierbar ist.

Bleibt noch die Frage, wie eigentlich der Zugriff auf die NSS erfolgt. Aus Linux-Sicht handelt es sich „nur" um ein Dateisystem mit besonders granularen Zugriffsberechtigungen. Damit Clients aber die NSS auf einem Linux-Server in der gleichen Weise wie auf einem NetWare-Server sehen, ist ein weiterer Dienst erforderlich, der NCP-Server. Bei NetWare ist dieser Teil des Betriebssystems und muss nicht extra eingerichtet werden. Beim OES for Linux muss man ihn zusätzlich installieren und konfigurieren. Danach können Clients aber auf den Linux-Server in der gleichen Weise wie auf einen NetWare-Server zugreifen.

2.3.2 Die Partitionierung unter Linux

Der erste Schritt bei der Einrichtung der NSS auf einem OES-Linux-Server ist die Partitionierung. Dabei gibt es eine spezielle Anforderung: Die NSS benötigen EVMS (Enterprise Volume Management System) statt LVM (Logical Volume Management) als Basis für das Volume-Management.



Gut integriert: Die NSS können beim OES for Linux einfach über YaST eingerichtet und konfiguriert werden.

Wenn die NSS direkt bei der Installation des Linux-Systems mit eingerichtet werden, kann man auch gleich EVMS mit einrichten. Werden die NSS auf einer getrennten Partition installiert, kann man ebenfalls EVMS nutzen. Die einzige wirkliche Herausforderung ist die nachträgliche Einrichtung von EVMS auf einem Boot-Volume. In der Praxis sollte man diese – in der Dokumentation von Novell umfassend beschriebene – Variante aber vermeiden.

Falls die NSS gleich bei der Installation eines OES-Linux-Servers installiert werden sollen, muss die vorgeschlagene Partitionierung angepasst werden, um dort einen von EVMS verwalteten Bereich zu schaffen. Die Standard-Partitionierung belässt nicht ausreichend freien, nicht partitionierten Platz auf dem Datenträger.

Falls die NSS noch nicht installiert sind, können sie über YaST nachträglich konfiguriert werden. Der Dienst findet sich dort im Bereich *System*. Nach seiner Auswahl erfolgt die automatische Installation und Konfiguration. Dabei sind keine speziellen Aspekte bezüglich der Partitionierung zu beachten. Vielmehr lassen sich anschließend mit den speziellen Tools des OES innerhalb des verfügbaren freien Platzes auf der Partition zusätzliche logische Volumes anlegen.

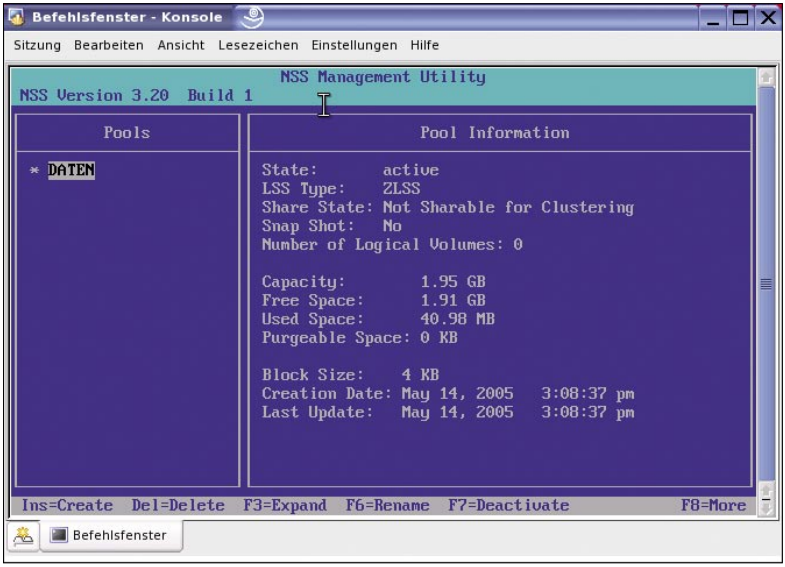
Zu beachten ist, dass man nicht gleichzeitig lokal mit OES-Tools und YaST arbeiten darf, da es ansonsten zu Zugriffskonflikten kommt. Man muss also YaST zunächst beenden, bevor man die weiteren Konfigurationsschritte durchführt.

2.3.3 Pools und Volumes

Die Erstellung von Pools und Volumes kann zum einen mit dem Novell iManager, zum anderen aber auch mit der NSSMU (NSS Management Utility) durchgeführt werden. Letztere hat den Vorteil, dass man damit direkt auf dem Server arbeiten kann. Sie arbeitet zeichenorientiert.

Dort muss zunächst das Gerät ausgewählt werden, auf dem die Partitionen, Pools und Volumes erstellt werden sollen. Im Hauptmenü kann auf die vorhandenen physischen Datenträger zugegriffen werden. Zu jedem Gerät werden die Informationen über den nicht partitionierten Plattenplatz angegeben. Wenn Sie einen zusätzlichen Datenträger erstellt und NSS erst später eingerichtet haben, müssen Sie *sdb* auswählen. Die weitere Steuerung erfolgt über die Funktionstasten am unteren Rand des Konsolenfensters.

Im ersten Schritt müssen Sie das Gerät für die Verwendung durch die NSS initialisieren. Durch diesen Schritt werden vorhandene Partitionen gelöscht. Anschließend können Sie den Befehl *Pools* im Hauptmenü wählen. Für diesen müssen Sie eine Partition erstellen. Dazu geben Sie zunächst den Namen des Pools an und wählen danach das – nun für die NSS vorbereitete – Gerät aus, auf dem der Pool angelegt werden soll. Im Anschluss können Sie die Partitionsgröße angeben. Der Pool und die zugehörige Partition werden dadurch erstellt. Ein Pool kann sich grundsätzlich über mehrere Partitionen erstrecken, ebenso wie eine Partition problemlos mehrere Pools enthalten kann.



Zeichenorientiert: Die NSSMU unter Linux ist ein Werkzeug für die schnelle und einfache Erstellung von Pools und Volumes für die NSS.

Danach können Sie in dem Pool Volumes erstellen. Dazu verwenden Sie den entsprechenden Menüpunkt im Hauptmenü der NSSMU. Erst nach der Erstellung eines Volumes können Benutzer mit den NSS arbeiten. Die Partitionsinformationen werden in YaST übrigens als EVMS-Partition angezeigt. Diese ist immer in */opt/novell/nss/mnt/.pools* gemountet. Konfigurationsänderungen können aber nur über die NSSMU oder den iManager, nicht aber mit YaST durchgeführt werden.

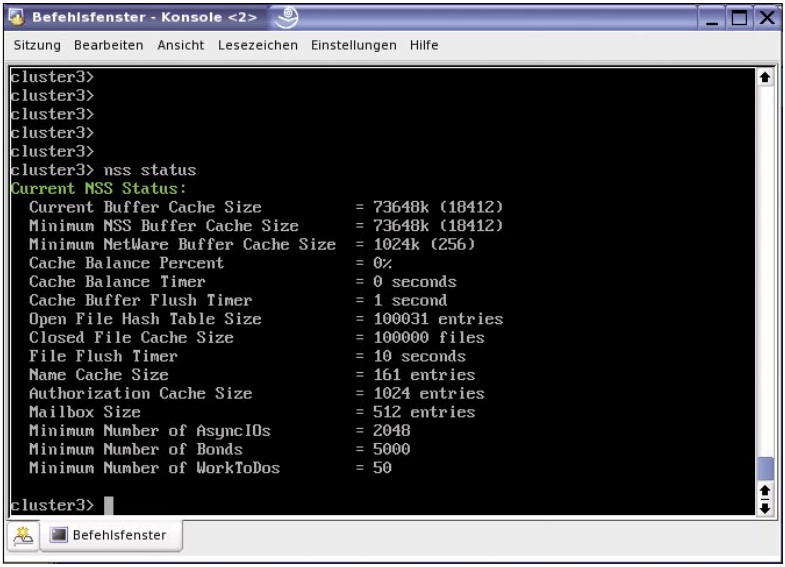
2.3.4 NSS nutzen

Zwei Tools für die Konfiguration der NSS wurden bereits vorgestellt. Neben der NSSMU und dem iManager gibt es noch die NSS Server Console. Dabei handelt es sich um eine Konsole, die einer NetWare-Server-Konsole ähnelt, aber nur NSS-Funktionen unterstützt. Sie wird mit */opt/novell/nss/sbin/nsscon* geladen. Die Konsole hat einen eigenen Prompt.

In dieser Konsole lassen sich nun die meisten NSS-Befehle nutzen. Eine Übersicht erhält man mit *nss help*. Einer der wichtigsten Befehle ist *nss status*. Er zeigt den aktuellen Konfigurationsstatus der NSS an. Weitere Befehle wie

- CacheStats
- FileCacheStats
- NameCacheStats

liefern detaillierte statistische Informationen zur Konfiguration und Nutzung der NSS. Die Cache-Statistiken sind wichtig, um zu erkennen, ob es ausreichend Cache gibt und ob das Dateisystem damit ausreichend performant arbeiten kann.



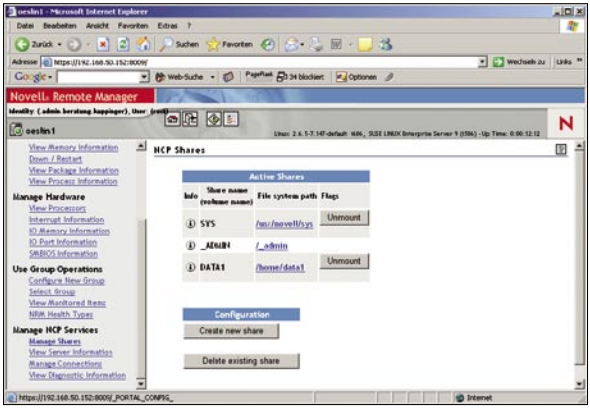
Wie bei der NetWare: Auch für die NSS unter Linux gibt es eine Konsole, über die wichtige Steuerungsbefehle eingegeben und ausgeführt werden können.

Im Gegensatz zur NetWare-Variante gibt es für die Linux-Version keine Startbefehle oder -parameter. Stattdessen muss man gegebenenfalls die Datei */opt/novell/nss/conf/nssstart.cfg* modifizieren. Dort lassen sich beispielsweise NSS-Befehle für die regelmäßige Pflege und Komprimierung von Volumes abspeichern.

Darüber hinaus gibt es noch einige spezielle Befehle wie *rights*, *attrib* oder *ravsui* für die Wartung. Sie sind in der Dokumentation der NSS for Linux umfassend erläutert und werden nur in Ausnahmefällen benötigt.

2.3.5 Der NCP-Server

Damit Novell-Clients auf die NSS eines Linux-Servers zugreifen können, ist aber noch ein weiterer Schritt erforderlich: die Einrichtung des NCP-Servers. NCP (NetWare Core Protocol) ist das Basisprotokoll für die Kommunikation mit Novells Server-Diensten. Es wird für die Authentifizierung ebenso wie für Fileserver-Zugriffe benötigt. Letztere erfolgen über das NFSP (NetWare File Sharing Protocol), dem zentralen Teil von NCP.



Volumes unter Linux: NCP-Volumes können über den Novell Remote Manager freigegeben werden. Die Clients sehen damit einen Linux-Server so wie bisher einen NetWare-Server.

Die Installation des NCP-Servers erfolgt entweder direkt bei der Einrichtung eines OES-Servers auf Linux-Basis oder später über YaST. Dort findet sich der NCP-Server als Option im Bereich System. Er kann mit oder ohne NSS installiert werden, wobei eigentlich nur die Verwendung mit den NSS Sinn macht, da diese die gleichen Sicherheitsfunktionen wie die (ebenfalls über NSS arbeitenden) Volumes auf NetWare-Servern bereitstellen.

Bei der Einrichtung eines NCP-Servers werden so genannte Volume Mount Points für die Standard-Verzeichnisstrukturen *public* und *login* erzeugt. Weitere Volume Mount Points können später über den Befehl *ncpcon* oder über den Novell Remote Manager (NRM) erstellt werden. Jeder Volume Mount Point ist für den Benutzer in der gleichen Weise sichtbar wie ein Volume auf einem NetWare-Server. Damit kann man sehr einfach eine Struktur erstellen, die den Benutzern beispielsweise nach der Migration von einem NetWare- auf einen OES-Linux-Server eine identische Arbeitsumgebung bietet. Im laufenden Betrieb wird *ncpcon* für die Verwaltung benötigt. Neben der Erstellung von Volume Mount Points bietet der Befehl beispielsweise Funktionen für die Abfrage statistischer Informationen und zum Aktivieren oder Deaktivieren von Volumes.

Insgesamt ist es Novell mit der Verbindung von NSS und NCP beim OES for Linux gelungen, eine hohe Kompatibilität zwischen den beiden Betriebssystemen zu erreichen – sowohl für die Administration als auch für die Nutzung.

Martin Kuppinger

tecCHANNEL-Links zum Thema	Webcode	Compact
Novells Dateisystem unter Linux	461053	S.98
Administration des Linux-Dateisystems	402469	–

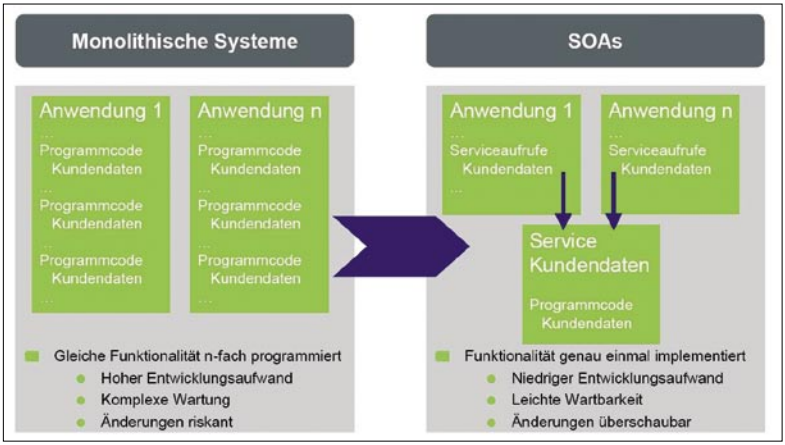
3. Grundlagen

Hinter Serviceorientierte Architekturen (SOA) steckt die Absicht, Geschäftsprozesse zu automatisieren und auf Maschine-zu Maschine-Kommunikation zu verlagern. Komplexe Anwendungen werden hierfür in standardisierte Services aufgebrochen und verteilt zur Verfügung gestellt. Die wichtigsten SOA-Basics stellen wir Ihnen in diesem Kapitel vor. Web Services sind eine mögliche Implementierung einer serviceorientierten Architektur (SOA) und sollen wesentlich zur Senkung der Integrationskosten für Internet-basierte Informationssysteme beitragen. Unser Grundlagenartikel beschreibt die Protokolle und Komponenten.

Der Ausfall wichtiger IT-Systeme kann für ein Unternehmen gravierende Folgen bis hin zur Existenzgefährdung haben. Standby-, Cluster- und fehlertolerante Server bieten Ausfallsicherheit auf verschiedenem Niveau. Unser Kostenvergleich zeigt, dass sich oft preiswerte Lösungen mittelfristig als kostspielig erweisen.

3.1 Serviceorientierte Architekturen – Grundlegende Konzepte

Derzeit ist die IT-Anwendungsentwicklung und der Betrieb von IT-Applikationen geprägt von monolithischen, siloartigen Systemlandschaften. Die beträchtlichen Investitionen in Wartung, Pflege und Betrieb der historisch gewachsenen Systeme nehmen mittlerweile bis zu 70 Prozent des IT-Budgets in Anspruch.



Unterschied: Der Nutzen von SOA im Vergleich zu traditionellen, monolithischen Systemen. (Quelle: Berlecon Research 2006)

Langfristig hat diese statische, teure IT kaum Zukunftschancen. Ein mögliches alternatives Konzept für eine dynamische, kostensenkende IT ist die serviceorientierte Architektur (SOA). SOAs sind ganz allgemein dadurch gekennzeichnet, dass sie die Flexibilität der IT erhöhen und somit die Kosten für Wartung, Pflege und Anpassung der IT an neue Anforderungen verringern.

Viele Unternehmen beginnen zurzeit damit, ihre IT auf serviceorientierte Architekturen umzustellen. Sie haben den Hauptnutzen der deutlich höheren Flexibilität erkannt und versuchen, ihn für eigene Zwecke umzusetzen. SOAs punkten jedoch noch mit weiteren Features. Durch die Kapselung von IT-Funktionen in voneinander unabhängigen Diensten lassen sich die Auswirkungen von Änderungen beispielsweise signifikant beschränken.

Darüber hinaus können Dienste in unterschiedlichen Anwendungskontexten wieder verwendet werden. Neue Dienste und Produkte können so schneller eingeführt und existierende Dienste schneller an neue Anforderungen angepasst werden. Kosten und Entwicklungszeiten sinken. Diese Flexibilität kann auch genutzt werden, wenn neue regulatorische Rahmenbedingungen erfüllt werden müssen.

3.1.1 SOAs – Merkmale im Überblick

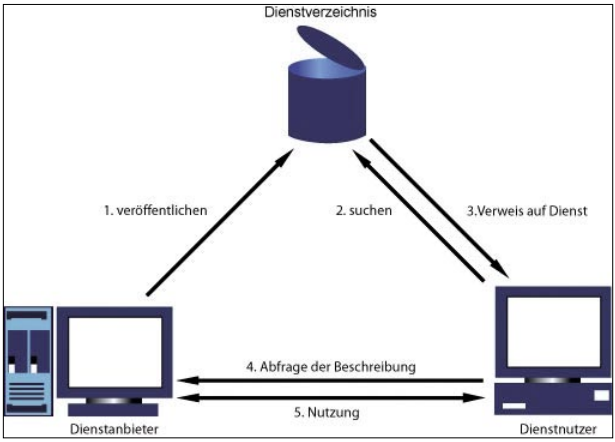
Serviceorientierte Architekturen lassen sich nur schwer fassen. Dies liegt daran, dass eine SOA keine konkrete Technik ist, sondern vielmehr eine abstrakte Software-Architektur. Im Zentrum steht das Anbieten, Suchen und Nutzen von Diensten über ein Netzwerk. Die Dienste werden dabei fast immer von Applikationen oder anderen Diensten genutzt. Welche Hardware, welche Software oder welches Betriebssystem dabei verwendet wird ist unerheblich.

Vom Standpunkt der Architektur aus betrachtet stellt eine SOA einen vollständigen Paradigmenwechsel in der IT dar: nicht mehr die Applikationen stehen im Vordergrund, sondern die Geschäftsprozesse. Wesentliches Merkmal einer SOA ist somit die Unabhängigkeit von den Details der Implementierung. Dienste sind lediglich „lose verkoppelt“. Damit ist gemeint, dass Dienste bei Bedarf dynamisch von Applikationen oder anderen Diensten gesucht und eingebunden werden. Dabei erfolgt die Einbindung zur Laufzeit. Oft ist zum Zeitpunkt der Übersetzung des Programms nicht bekannt, was zur Laufzeit aufgerufen wird.

Damit die Dienste gefunden werden können, gibt es einen Verzeichnisdienst oder ein Repository, in dem die Dienste registriert sind. Um die Dienste zu suchen und vor allem zu nutzen, muss der Aufrufer sich mit diesen unterhalten können. Dies geht nur über maschinenlesbare Schnittstellen, die offenen Standards genügen. Es muss also eine so genannte „Service Description“ in maschinenlesbarer Form vorliegen. Zulässig sind dann nur Zugriffe über diese Schnittstelle.

In jedem Fall erfolgt die Kommunikation innerhalb einer SOA vollständig automatisiert. Ein Mensch kann sie zwar anstoßen, die Bearbeitung geschieht aber unabhängig von ihm und automatisch. Ein Beispiel für einen SOA-gesteuerten Pro-

zess ist die automatische Überweisung eines Geldbetrages, sobald der Kontostand des Zielkontos unter einem bestimmten Betrag fällt. Solche Architekturen werden auch als ereignisgesteuert bezeichnet.



Dreierpack: Das magische SOA-Dreieck zeigt das Zusammenspiel der wichtigsten Beteiligten. (Quelle: Dostal et al: Serviceorientierte Architekturen mit Web Services, Elsevier/Spektrum)

Grundsätzlich gibt es in einer SOA drei Beteiligte: Den Anbieter des Dienstes, den Nutzer und den Vermittler. Die Grafik zeigt das Zusammenspiel der drei Akteure – das „magische SOA-Dreieck". Die drei Elemente werden in den folgenden Abschnitten ausführlicher beschrieben.

3.1.2 SOA-Dienste

Wie kann man sich einen SOA-Dienst konkret vorstellen? Im einfachsten Fall lässt sich ein Dienst als Weiterentwicklung von PlugIns auffassen. PlugIns haben ebenfalls eine eindeutige Schnittstelle und eine für den Anwender unsichtbare Implementierung. Sie erweitern die Anwendung um bestimmte Funktionen, die bei der Programmerstellung noch nicht geplant waren.

Anders als bei SOA-Diensten liegen bei PlugIns die Schnittstellen aber meist nicht in maschinenlesbarer Form vor und sie nutzen meist nur eine einzige, sehr starre Schnittstelle. Bei SOA ist das anders. Im Zusammenhang mit Web Services hat sich bei SOA die Web Service Description Language (WSDL) als Beschreibungssprache für solche Schnittstellen durchgesetzt und SOAP als Standard für Nachrichten. Obgleich WSDL und SOAP an unterschiedliche Transportmechanismen gebunden werden können, werden sie häufig mit synchroner Kommunikation über HTTP assoziiert: ein Client schickt einen Request an einen Server und erhält ein Reply zurück. In vielen Kontexten ist aber eine asynchrone Kommunikation über Messages und Queues vorteilhafter – aus diesem Grund hat sich auch MOM

(Message Oriented Middleware) als ein Integrationsparadigma etabliert. Bei asynchroner Kommunikation dominiert inzwischen JMS (Java Message Service).

Viele SOA-Plattformen unterstützen ein breites Spektrum an Austauschformaten, so dass Anwender im Einzelfall entscheiden können, welches Format für den jeweiligen Anwendungsfall am geeignetsten ist. Der Enterprise Service Bus fungiert dann als Bindeglied und Kommunikationsinfrastruktur. Wird eine SOA-Plattform zur Verfügung gestellt, muss diese konkret betrieben und gewartet werden. Der Diensteanbieter muss die Verfügbarkeit garantieren. Dazu gehören oft Aufgaben, die in der Regel in Rechenzentren geleistet werden wie Backups oder Wartung.

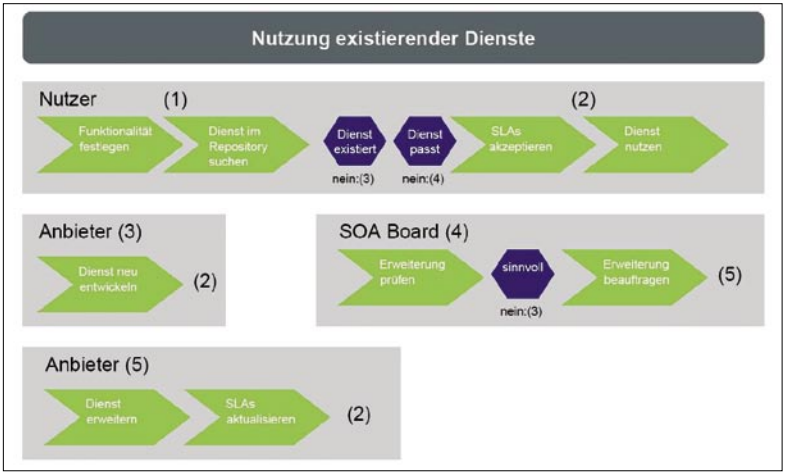
Sicherheit ist ebenfalls ein Punkt, den der Servicebetreiber abdecken muss. Dazu gehören Aufgaben wie Authentifizierung und Authentisierung. Bei der Authentifizierung prüft der Diensteanbieter, ob der Aufrufer auch derjenige ist, der er zu sein behauptet. Die Authentisierung stellt sicher, dass der Aufrufer auch berechtigt ist, die Funktionalität zu nutzen, die er gerade aufruft. Die beschriebenen Aufgaben gelten für alle Dienste – auch für diejenigen, die der Diensteanbieter gar nicht selbst anbietet, sondern etwa über das Netz nutzt.

3.1.3 Dienstverzeichnis und -nutzer

Dienste müssen verzeichnet werden, um von einem potenziellen Nutzer gefunden zu werden. Bei der Entwicklung neuer Anwendungen kann dann einfach festgestellt werden, welche Dienste vorhanden sind und genutzt werden können. Hierzu dient ein Dienstverzeichnis, auch Registry oder Repository genannt. In einer einfachen SOA muss jeder Anbieter selbst aktiv seine Dienste bei einem solchen Verzeichnis registrieren. Künftig könnten solche Aufgaben auch Suchmaschinen erledigen. Mit UDDI (Universal Description, Discovery and Integration) existiert seit Jahren ein Registry-Standard, der aber bisher nur vereinzelt in der Praxis eingesetzt wird. Viele Unternehmen verwenden stattdessen ein selbst entwickeltes Repository für die zentrale Bereitstellung von Informationen über Dienste.

Die Güte eines Verzeichnisses steht und fällt mit den Kategorien. Für eine gute Klassifizierung ist es nötig, dass jeder Dienst genau einer Kategorie eindeutig zugeordnet ist. Damit die SOA akzeptiert wird und möglichst einfach gehandelt werden kann, sollte die Suche nach Diensten für einen Nutzer von einem normalen Diensteaufruf nicht zu unterscheiden sein. Praktisch wird es bei den Diensten keine Monopole geben, sondern eine Vielzahl von Dienste-Verzeichnissen. Viele Firmen werden mindestens eine Instanz für ihre Internet-Angebote haben und eventuell eine zweite für den internen Zugriff. Ferner kann es weitere Installationen für einzelne Bereiche geben.

Der Dienstenutzer muss dem Diensteanbieter nicht bekannt sein. Für ihn ist es wichtig, dass Standards vorhanden sind und vor allem auch eingehalten werden. So muss der Dienst fähig sein, dem Nutzer seine Schnittstelle vollständig darzulegen. Danach findet die Kommunikation über ein Protokoll statt, das beiden bekannt sein muss. Ein Beispiel für ein solches Protokoll ist SOAP.



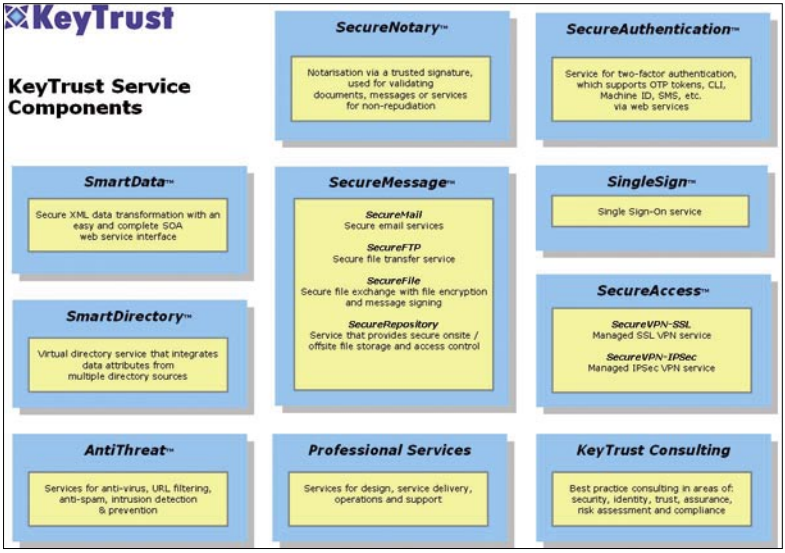
SOA: Ein grober Prozess zur Nutzung existierender Dienste. (Quelle: Berlecon Research 2006)

3.1.4 Ausführbare Aktionen

Das Zusammenspiel zwischen Dienstanbietern, Dienstnutzern und Dienstverzeichnis muss gut funktionieren. Denn eine ganze Reihe von Aktionen können in einer solchen Umgebung ausgeführt werden. Eine erste solche Aktion ist die „Veröffentlichung" eines Dienstes. Der Eintrag und die Anmeldung in einer Registry reichen hierfür nicht aus. Der Dienst muss vorher in einer entsprechenden Umgebung installiert werden – ein Vorgang, der als „Deployment" bezeichnet wird. Erst anschließend sollte der Dienst registriert werden.

Die zweite Aktion ist die des „Suchens" nach Diensten. Die Frage stellt sich, wie man nach einem Dienste suchen kann. Bei Diensten gibt es keine guten Quellen, die eine Suchmaschine analog etwa zu Websites durchsuchen kann. Wichtig ist daher, dass für jeden Dienst eine gute Beschreibung erstellt wird. Dies wird meist auf Basis von Taxonomien oder Ontologien vorgenommen. Vereinfacht kann man sich ein solches Verzeichnis wie die Gelben Seiten vorstellen – für verschiedene Kategorien gibt es eine Liste von möglichen Diensten.

Ist der Dienst gefunden, so ist eine weitere Aktion möglich: Die Aushandlung, wie mit dem Dienst zu interagieren ist. Dazu wird zunächst die Schnittstellenbeschreibung des Dienstes abgefragt. Unter Umständen ist der Dienst nur unter bestimmten Voraussetzungen nutzbar – etwa der eines Zertifikats oder der Authentifizierung. Dazu müssen entsprechende Richtlinien ausgetauscht werden. Erfolgt eine Einigung, so spricht von einer erfolgreichen „Bindung" an einen Dienst.



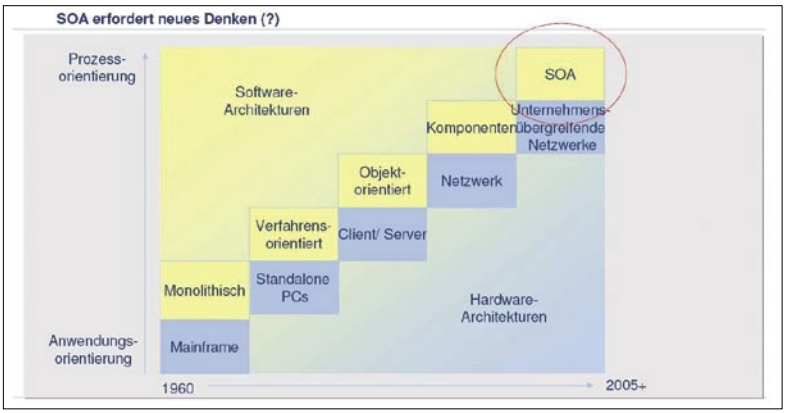
Beschreibung: Beispiel für eine mögliche Taxonomie eines Anbieters von Sicherheitsdiensten. (Quelle: KeyTrust)

3.1.5 SOA – ein neues „Programmierkonzept“

In mancherlei Hinsicht erinnert SOA an entfernte Funktionsaufrufe, so genannte Remote Procedure Calls (RPCs). Zwar werden Web Services, eine der Umsetzungen von SOA, oft als einfache RPCs verwendet. Die Nutzung des SOA-Konzepts geht aber wesentlich weiter und ist das derzeit letzte Glied in einer Reihe von Programmierkonzepten. Zur Erinnerung und zum Verständnis von SOA ein paar wichtige Pfeiler moderner Programmierkonzepte.

Die prozedurale Programmierung wurde entwickelt, um dem schlecht wartbaren Spaghetti-Code aus den Anfängen der Software-Entwicklung Herr zu werden. Dazu wurde das Modulkonzept eingeführt, das die Verteilung eines Programms auf mehrere Dateien und damit eine übersichtliche Strukturierung und die Erstellung von Bibliotheken ermöglichte. Mit der prozeduralen Programmierung wurde es vor allem aber möglich, einzelne Funktionalitäten zu kapseln und an beliebigen Programmstellen durch einen Aufruf zu nutzen.

Als Nachfolger der prozeduralen Programmierung entstand Mitte der 80er Jahre die objektorientierte Programmierung – Folge der stetig zunehmenden Komplexität der Programmentwicklung. Die objektorientierte Programmierung erlaubte eine deutlich bessere Strukturierung und eine brauchbare Wiederverwendung.



Im Lauf der Zeit: Die Entwicklung vom Mainframe bis zum modernen SOA im Überblick. (Quelle: Quelle: plenum Management Consulting GmbH 2005)

Doch auch die objektorientierte Programmierung war nicht der Weisheit letzter Schluss. Objekte sind in vielen Fällen zu feingranular und schränken die verwendete Sprache und Umgebung sehr stark ein. Den nächsten Schritt bildeten deshalb die serviceorientierten Architekturen.

3.1.6 SOA-Anwendungen

Bei der Einführung einer SOA hat sich ein schrittweises Vorgehen bewährt, bei der Abteilungen und Anwendungen nach und nach auf die SOA umgestellt werden. Dies verringert den organisatorischen Aufwand und vermindert das Risiko des Scheiterns. Besonders geeignet für initiale SOA-Projekte sind

- Anwendungen, für die Abteilungen zuständig sind, die der SOA-Idee positiv und aufgeschlossen gegenüber stehen;
- die vergleichsweise einfach zu realisieren bzw. auf SOA umzustellen sind, also mit wenig Risiko verbunden sind;
- die eine hohe Sichtbarkeit garantieren, z.B. weil sie von vielen anderen Abteilungen genutzt werden oder eine für das Unternehmen zentrale Funktionalität bereitstellen.

Die Entwicklung einer SOA-Anwendung läuft typischerweise folgendermaßen ab: Als erstes werden typische Szenarien festgelegt und in Form von Fallstudien festgehalten. Diese werden als Ablaufdiagramm modelliert. Dabei werden die Prozesse, die in den typischen Anwendungsfällen ablaufen, festgehalten und präzisiert. Im dritten Schritt werden dann die einzelnen Prozessschritte genauer herausgearbeitet. Diese einzelnen Komponenten sind die Dienste oder Services, die an externe Partner vergeben werden können.

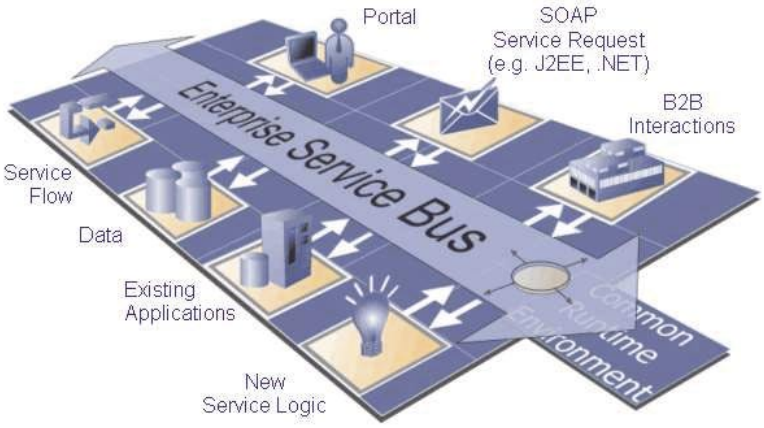
Ein Wort noch zu SOA und ASP: SOA hat einiges mit ASP-Anwendungen gemein, unterscheidet sich davon jedoch auch. Bei ASP liegt die ganze Anwendung bei einem Anbieter und kann extern von einem Nutzer aufgerufen werden. Anders als bei SOA ist es bei ASP aber immer eine ganze Anwendung, während bei SOA Teile aufgerufen werden.

Ein Beispiel ist eine Office-Anwendung. Nutzt man einen Editor kann man bestimmte Zusatz-Funktionalitäten verwenden, die der Editor selbst nicht anbietet. Beispielsweise eine Rechtschreibkontrolle, Zeichenformatierung oder Import- und Export-Filter. Wird beispielsweise die Rechtschreibkontrolle aufgerufen, so wird nach dem obigen Schema in einem Verzeichnis nach einem solchen gesucht, diese gefunden und genutzt. Was im Hintergrund abläuft, merkt der Nutzer nicht.

Langfristig könnten SOA-Anwendungen das Ende der heutigen Applikationen sein, wobei entsprechenden Abrechnungsmodelle installiert werden müssten. Statt monolithischer Anwendungen dürften in jedem Fall in Zukunft mehr komponentenbasierte Systeme entstehen.

3.1.7 Enterprise Service Bus

Eine zentrale Rolle im SOA-Konzept nimmt der Enterprise Service Bus (ESB) ein, wobei zwei Interpretationen üblich sind. Ein Teil der Experten interpretiert ESB als Bestandteil einer SOA. Nach dieser Interpretation wird die Kommunikation in der SOA über eine zentrale Komponente mit intelligenten Routing-Fähigkeiten vorgenommen. Dieser Verteiler wird dann als ESB bezeichnet.



Datenautobahn: Der Enterprise Service Bus nimmt eine wichtige Rolle in SOA ein. (Quelle: IBM)

Danach ist die zentrale Aufgabe eines ESB der Austausch von Daten zwischen IT-Systemen oder Teilen von IT-Systemen. Der Datenaustausch findet dabei in Form von Service-Aufrufen statt. Der ESB kann als zentraler Server existieren („Hub-and-Spoke-Ansatz"), als vollständig dezentrale Umsetzung oder auch als föderiertes System, das heißt als Verbindung mehrerer Zentralsysteme. Zusätzlich kann ein ESB zentrale Dienste anbieten wie eine Registry, Single-Sign-On, Verschlüsselungsdienste und Datenkonvertierung.

Der andere Teil der Experten interpretiert den ESB als logische Weiterentwicklung von SOA. Der Hintergrund ist, dass der Datenstrom in Unternehmen immer von Ereignissen gesteuert wird – man spricht daher auch von „Event driven Enterprises". Um ein ereignisgetriebenes Unternehmen in der IT umzusetzen, braucht man Eigenschaften der SOA wie lose Kopplungen. Der kritische Datenfluss wird vom ESB übernommen.

3.1.8 Fazit

Viele Unternehmen beginnen zurzeit damit, ihre IT auf serviceorientierte Architekturen (SOAs) umzustellen. Die Vorteile liegen eindeutig in einer deutlich höheren Flexibilität der IT. Neue Dienste und Produkte können so schneller eingeführt und existierende Dienste schneller an neue Anforderungen angepasst werden. Kosten und Entwicklungszeiten sinken.

Damit haben SOAs das Potenzial, das nächste bedeutende Paragdigma der Informatik zu werden. So wie etwa die objektorientierte Programmierung gegenüber der prozeduralen Programmierung ein höheres Abstraktionsniveau eingeführt hat, so gestatten SOAs eine weitere, abstrakte Sicht auf ansonsten sehr komplexe Phänomene. Dies ermöglicht meist, die hohe Komplexität der Unternehmens-IT besser zu bewältigen und flexible und wieder verwendbare Architekturen zu entwickeln. Der derzeit mit Abstand vielversprechendste Ansatz, das SOA-Konzept umzusetzen, sind die Web Services.

Dr. Klaus Manhart

tecCHANNEL-Links zum Thema	Webcode	Compact
Serviceorientierte Architekturen – Grundlegende Konzepte	456248	S.105
Web Services – Grundlagen, Aufbau und Struktur	457051	–
In zehn Schritten zur SOA	569662	–
SOA durch Technik-Angst und mangelndes Wissen gebremst	816629	–
Business Intelligence-Projekte optimal umsetzen	434480	–

3.2 Web Services – Grundlagen, Aufbau und Struktur

Web Services sind eine Realisierung einer SOA, mit der sich Informationsdienste im WWW automatisieren lassen. Es handelt sich dabei um funktionale Dienste, die über Internetprotokolle und die Internet-Infrastruktur übertragen werden können. In den meisten Fällen sind Web Services Software-Komponenten, die mittels Applikationsserver im Internet „nutzbar" gemacht werden. Um Daten miteinander auszutauschen, werden XML-basierte Standards verwendet. Etwaige Transaktionen können ohne menschliches Zutun automatisch zwischen Web-Services abgewickelt werden.

Die lose Kopplung der Komponenten über Web Services führt zu einer diensteorientierten SOA-Architektur, in der die funktionale Schnittstelle und ihre Semantik die Integration zur Gesamtlösung bestimmt. Die SOA von Web-Services besagt, dass Web Services beschrieben, veröffentlicht (published), gefunden (discovered) und dynamisch aufgerufen (invoked) werden können.

3.2.1 Beispiele für Web Services

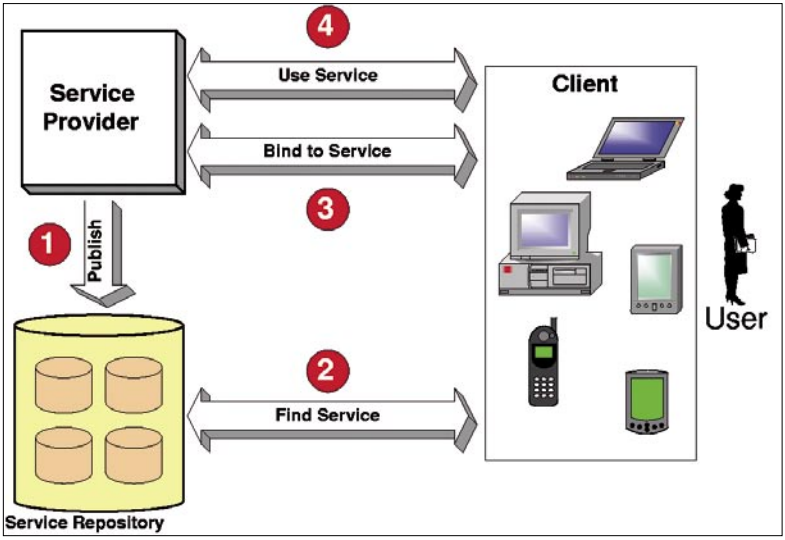
Die mit Web Service Diensten verbundenen Protokolle und Standards wie SOAP, WSDL und UDDI bilden den technologischen Rahmen für die Realisierung solcher Szenarien in verteilten Anwendungen. Das W3C hat eine eigene Arbeitsgruppe eingerichtet, die sich mit der Frage der Web-Services-Architektur und den entsprechenden Szenarien auseinandersetzt. Web Services haben sich nun schon seit einiger Zeit bei der Integration bewährt und etabliert und spielen nicht nur im Bereich unternehmensweiter „großer" Lösungen eine Rolle. Sie haben mittlerweile auch die Hardware-, Lösungs- und Anwendungsebene durchdrungen. Im Bereich der Anbindung mobiler Geräte und dedizierter Hardware (embedded devices) erleichtern Web Services die Integration in Anwendungen signifikant.

Seit 2002 gibt es von Google einen Web Service, der durch seine Funktionalität die gleichen Möglichkeiten der Website anbietet, wie die Benutzerschnittstelle auf der Website selbst (http://code.google.com/). Programme können nun mit einem Ansprechen der Schnittstelle direkt nach Informationen im Internet suchen, erhalten über die Schnittstelle die Ergebnisdaten und können diese für ihre eigenen Aufgaben verwenden. Das Parsen der Google-Webseite ist dazu keine auch nur annähernd gleichwertige Alternative.

Weitere Beispiele

Ein weiteres Beispiel ist die Interaktion zwischen Fluggesellschaften und Reisebüros. Die Fluggesellschaften stellen Möglichkeiten zum Nachschlagen bzw. Buchen von Flügen über einen Web Service bereit. Die Reisebüros bieten auf ihrer Webpräsenz Flüge verschiedener Fluggesellschaften an, von denen die Reisebü-

ros zur Laufzeit über den Verzeichnisdienst UDDI erfahren. Der Kunde kann auf der Webpräsenz des Reisebüros nun zentral Preise und Termine verschiedener Flüge vergleichen und direkt buchen.



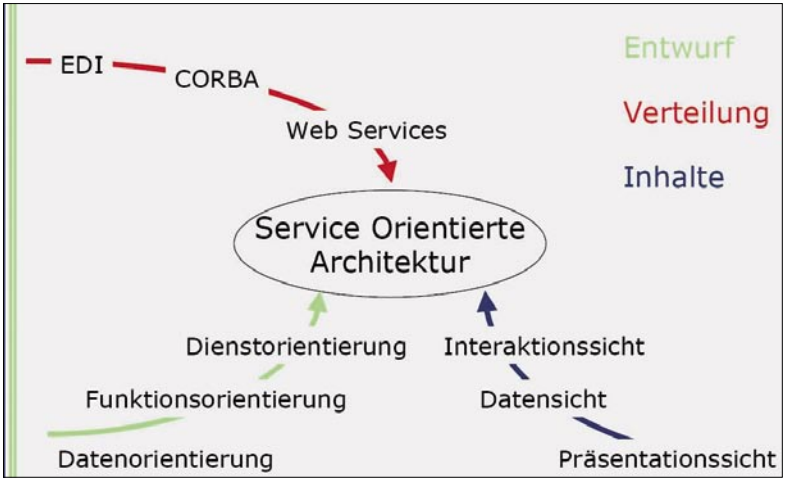
Grundprinzip von Web Services: Ein Dienstanbieter veröffentlicht einen Service in einem Dienstverzeichnis (1). Ein User findet den Service (2), bindet ihn in seine IT ein (3) und nutzt ihn (4). (Quelle: Fraunhofer-Institut für Angewandte Informationstechnik)

Web Services sind nicht die erste Realisierung einer SOA. Schon vor Web Services existierten eine Reihe von Konzepten, die ähnliche Probleme erfolgreich gelöst haben. Das war zum Beispiel COM/DCOM von Microsoft (www.microsoft.com/com), RMI von Sun (http://java.sun.com/rmi/) und Corba von OMG (www.omg.org/corba-corner/). Von diesen drei Konzepten war allerdings lediglich Corba plattformunabhängig, die anderen waren gebunden an das Betriebssystem des jeweiligen Herstellers. Kern der 1991 veröffentlichten Corba-Spezifikation war das Objektmodell. Corba setzte sich letztendlich deshalb nicht durch, weil es mit verschiedenen Problemen kämpfte – etwa unvollständiger Spezifikation oder unbefriedigender Abbildung der Datentypen in andere Programmiersprachen.

3.2.2 Merkmale von Web Services

Eine allgemeine, einheitliche Beschreibung von Web Services ist schwierig. Trotzdem herrscht in Standardisierungsgremien wie dem W3C eine allgemeine Übereinstimmung darüber, was ein Web Service ist:

- So sind Web Services immer über programmierbare Schnittstellen erreichbar und mittels Nachrichten-basiertem XML-Datentransfer wie SOAP und WSDL aufrufbar („Programmierbarkeit“).



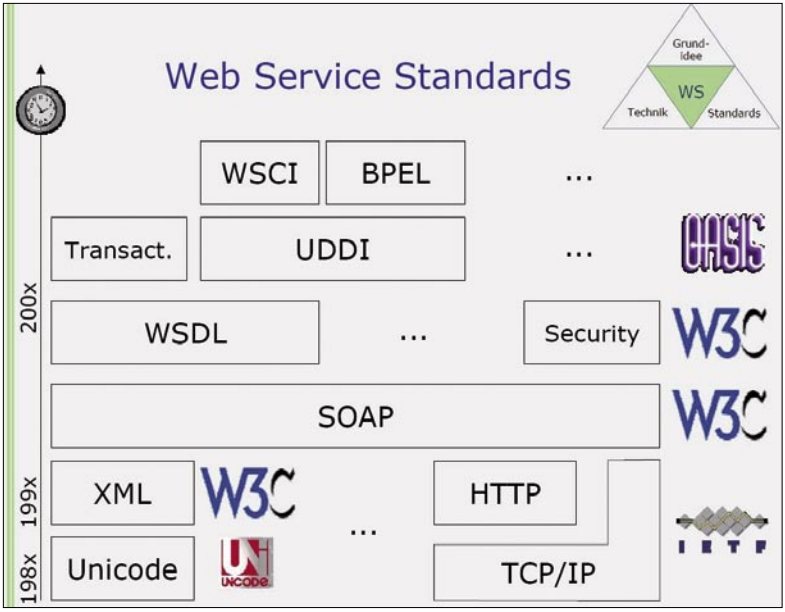
Web Services: nur eine mögliche Realisierung von SOA (Quelle: jeckle.de)

- Ein Web Service basiert auf der Internet-Protokollsuite. Operationen und Nachrichten können mehrere Protokolle unterstützen, z.B. das Hypertext Transfer Protocol (HTTP) oder das Simple Mail Transfer Protocol (SMTP) („Protokolltransparenz“).
- Web Services sind zudem unabhängige, in sich abgeschlossene bzw. gekapselte Anwendungen, die eine genau definierte Aufgabe erfüllen („Kapselung“). Die Implementierungsdetails bleiben Konsumenten und Anbietern verborgen („lose Koppelung“).
- Web Services können entweder in weitere Web Services zerlegt werden oder mehrere, wieder verwendbare Basis-Web-Services können zu einem neuen Web Service zusammengestellt werden („Komposition“).
- Web Services sind ortsunabhängig und können jederzeit und von jedem Ort aus aktiviert werden, vorausgesetzt Benutzer und Anwendungen haben entsprechende Zugriffsrechte („Ortstransparenz“). Begleitet wird ein Web Service von Metadaten, die während der Laufzeit von weiteren Web Services ausgewertet werden können („Selbstbeschreibung“). Name, Beschreibung, Version und Dienstgüte sind typische Beschreibungsmerkmale.
- Darüber hinaus können Web Services entweder von informativer oder von transaktioneller Natur sein. Transaktionelle Web Services können Bestandteil lang laufender Geschäftstransaktionen sein.

3.2.3 Basiskomponenten von Web Services

Die Standardisierung und Automatisierung von Web Services lässt sich nur zu einem bestimmten Teil vorantreiben. Das bekannte Dilemma zwischen Dejure- und Defacto-Standards bleibt bislang noch bestehen.

Das World Wide Web Consortium (W3C), OASIS (Organization for the Advancement of Structured Information Standards) und einige weitere unabhängige Gremien widmen sich der Standardisierung in diesem Bereich. Das W3C konzentriert sich hierbei weitgehend auf horizontale Standards, das heißt, technische Standards, die auf alle Industriezweige angewendet werden können. OASIS dagegen befasst sich mit so genannten vertikalen Standards und verwendet – soweit möglich – bestehende technische Standards.

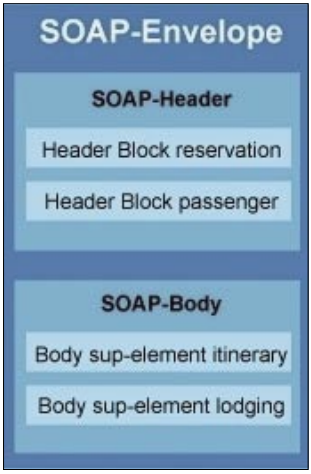


Standards: Die wichtigsten Standards bei Web Services im Überblick. (Quelle: jeckle.de)

Folgende Standards bilden das Fundament der Web-Service-Architektur:

SOAP

SOAP („Simple Object Access Protocol“) ist das XML-basierte Format zur Kommunikation und zum Nachrichtenaustausch und dessen Einbettung in ein Transportprotokoll. Der Standard definiert allgemeine Regeln zum Austausch von Nachrichten zwischen Applikationen.



SOAP-Nachricht: Aufbau (Quelle: Dustdar Schahram u.a.: Software-Architekturen für Verteilte Systeme, Springer, 2003)

SOAP übernimmt die lose Koppelung, die verteilte Architektur und den Transport über bekannte Internet-Protokolle – unabhängig von der zu Grunde liegenden Software-Architektur. Dem Thema SOAP widmet sich ein eigener Beitrag, der Ende Januar erscheinen wird.

WSDL

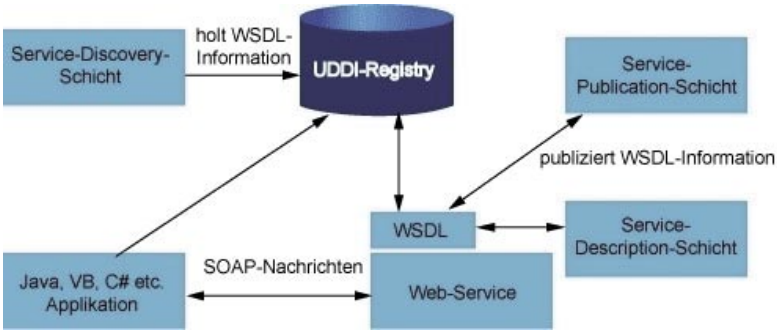
WSDL („Web Service Description Language“) ist eine XML-basierte Beschreibungssprache, um Web Services bzw. deren Fähigkeiten zu beschreiben. Genau genommen werden die Schnittstellen von Web Services beschrieben, nicht die Services selbst. Strukturell betrachtet, besteht ein WSDL-Dokument aus einem in XML beschriebenen Schema. In diesem Schema ist eine Grammatik enthalten, mit der Verträge („contracts“) formuliert werden können. Diese Verträge haben ihre Gültigkeit bei der Kommunikation zwischen zwei Endpunkten. Zu WSDL veröffentlichen wir demnächst einen eigenen Beitrag.

UDDI

UDDI („Universal Description, Discovery and Integration“) ist ein Verzeichnisdienst für Web Services. Der Dienst spezifiziert eine standardisierte Verzeichnisstruktur für die Verwaltung von Web-Services-Metadaten. Es handelt sich dabei um eine Art „Gelbe Seiten“ (yellow pages), in dem Web Services und ihre Schnittstellen registriert sind. Zu den Metadaten gehören allgemeine Anforderungen, Web-Services-Eigenschaften oder die benötigten Informationen zum Auffinden von Web Services. Die White-Pages bieten Aufschluss über den Firmennamen, Beschreibung und Ansprechpartner. Die Yellow-Pages enthalten Produkt, Dienst, Industriezweig und geographische Unterteilung, während sich die Green-Pages mit den technischen Details der Datenkommunikation auseinander setzen.

UDDI ist zwar nicht unbedingt notwendig für den Einsatz von Web Services, gehört aber als Infrastrukturkomponenten unbedingt zu einer SOA. UDDI unterscheidet sich von den anderen beiden Spezifikationen darin, dass zur Beschreibung eines Verzeichnisdienstes keine eigene XML-Anwendung verwendet wird. Allerdings sollte ein entsprechender Verzeichnisdienst mit WSDL-Dokumenten umgehen können und selbst auch als Web Services verfügbar sein.

Die folgende Grafik zeigt das Zusammenspiel der drei Standards:



Zusammenspiel: SOAP, UDDI und WSDL. (Quelle: Dustdar Schahram u.a.: Software-Architekturen für Verteilte Systeme, Springer, 2003)

Die im SOA-Beitrag (**Webcode 456248**) erwähnte Dreiecksbeziehung zwischen Diensteanbieter, -nutzer und –verzeichnis lässt sich nun auf die Basiskomponenten konkretisieren.

3.2.4 Rollen und Aktionen

Eine SOA-Architektur setzt drei Rollen voraus_

- **Dienstnutzer (Konsument):** Er agiert mittels XML-basierter Nachrichten und Transportprotokollen mit einem Web-Service-Verzeichnis oder -Anbieter. Die dynamische Anbindung mit dem kommunizierenden Web-Service erfolgt über ein Web-Service-Verzeichnis.
- **Dienstanbieter:** Er bietet einen Dienst über programmierbare Schnittstellen an.
- **Dienstverzeichnis (Repository):** Es enthält eine logische Beschreibung und Angaben über den Aufenthaltsort sämtlicher Web-Service-Anbieter.

Konsument, Anbieter und Verzeichnis sind austauschbar. Ein Konsument kann auch als Zwischenhändler fungieren und somit auch Anbieter eines Web-Service sein. In ihrer einfachsten Form interagieren zwei Web-Services wie folgt:

1. Ein potentieller Nutzer eines Web-Service stellt eine Suchanfrage an einen Verzeichnisdienst.

2. Das Web-Service-Verzeichnis enthält eine kategorisierte Ansammlung von registrierten, vertrauenswürdigen Web Services.

3. Nachdem der gewünschte Service ausfindig gemacht wurde, können weitere Details über Nachrichtenformate und Protokolle angefragt werden.

4. Basierend auf der Servicebeschreibung, kann eine Protokollanbindung erzeugt werden. Somit können beide Web Services miteinander kommunizieren.

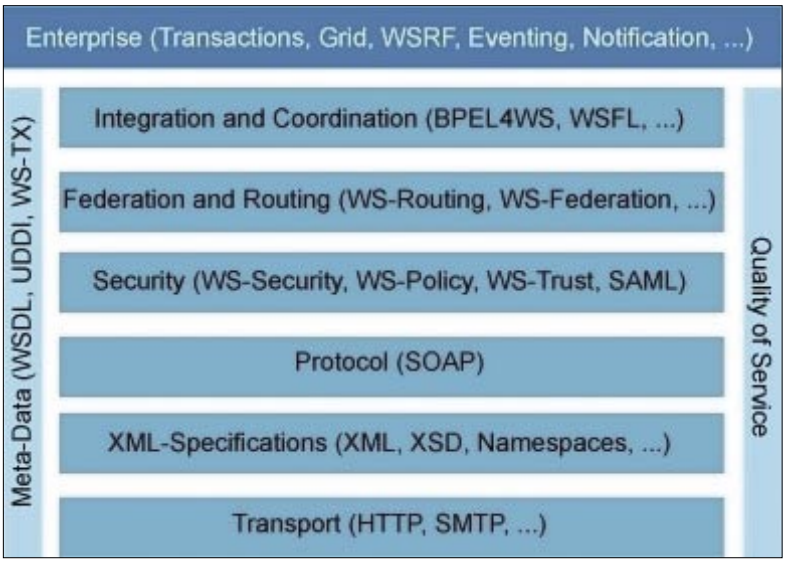
Technisch gestaltet sich der Ablauf wie folgt: Ein Anbieter, der einen Dienst in Form eines Web Services anbieten möchte, erstellt von diesem zunächst eine WSDL-Schnittstellenbeschreibung in Form eines entsprechenden XML-Dokuments. Dieses WSDL-Dokument wird publiziert, indem es ganz oder in bestimmten Teilen zu einem UDDI-basierten Verzeichnisdienst transferiert wird. Anschließend wartet der Diensteanbieter, bis ein Dienstnutzer einen entsprechenden Dienst sucht. Laut Spezfikation müssen UDDI-Implementierungen zu diesem Zweck eine SOAP-Schnittstelle zur Verfügung stellen. Diese wird vom UDDI-Gremium mittels WSDL-Dokumenten beschrieben.

Hat der Dienstnutzer einen geeigneten Web Service gefunden, so fordert er die Schnittstellenbeschreibung, also das WSDL-Dokument, an. Der Verzeichnisdienst liefert hierzu eine Referenz (URI) auf das WSDL-Dokument. Das fordert der Nutzer in einem weiteren Schritt an. Danach werden mit Hilfe der WSDL-Beschreibung die Programmteile erzeugt, welche die Anwendung des Nutzers in die Lage versetzt, mit der Anwendung des Dienstanbieters via SOAP zu kommunizieren.

3.2.5 Web Services Stack – das Schichtenmodell

Für eine vollwertige SOA-Implementierung müssen mehrere Anforderungen an einen so genannten SOA-Tempel realisiert werden. Diese werden üblicherweise in einem Schichtenmodell oder Stack, dem Web Service Stack, dargestellt. Der auf der folgenden Seite abgebildete Stack ist nur ein Stack unter vielen möglichen. Die Vielzahl möglicher Varianten lässt sich durch die verschiedenen Interessen und Betrachtungsweisen eines Stacks erklären. Begonnen wird bei einem Stack üblicherweise auf der untersten Ebene mit der Transportschicht. Dadurch kann ausgedrückt werden, dass Web Services nicht an ein bestimmtes Transportprotokoll gebunden sind. Verwendbar sind ganz unterschiedliche Protokolle wie http oder SMTP, die alle XML-Nachrichten transportieren können.

Die nächste Schicht und damit die Grundlage des gemeinsamen Datenmodells bilden XML- und XML-verwandte Technologien wie Schemata oder Namespaces. Die Protokolle zum Nachrichtenaustausch basieren wie die Nachrichten auf XML. Deswegen findet sich auf der folgenden Protokoll-Schicht die SOAP-Spezifikation. Sie beschreibt die Struktur und Semantik der zu verwendenden XML-basierten Nachrichten. Die fünfte Schicht Federation and Routing verfeinert die Konzepte für den Einsatz in verteilten Systemumgebungen und regelt das Zusammenspiel der Spezifikationen untereinander im Kontext jeweils eines Web Services.



Web Service Stack: Das Schichtenmodell für Web Services (Quelle: Dostal et al: Serviceorientierte Architekturen mit Web Services, Elsevier/Spektrum)

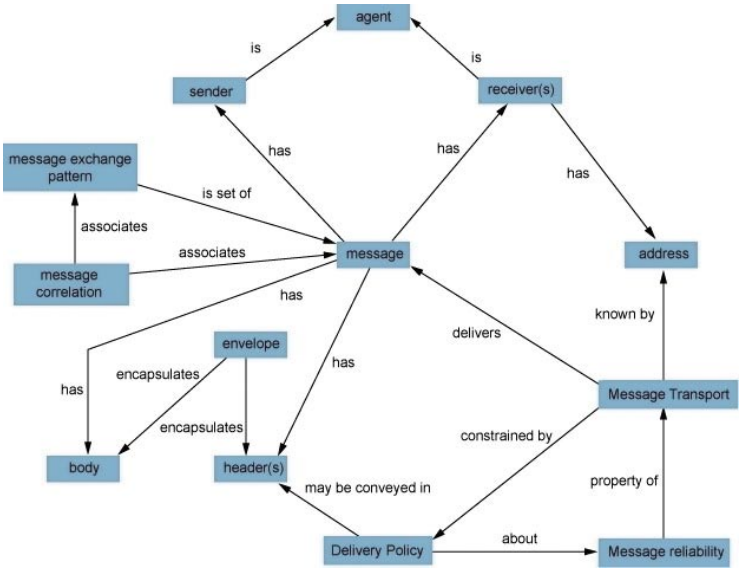
Das Zusammenspiel mehrere Web Services wird durch Spezifikationen auf einer weiteren, darüber liegenden Schicht beschrieben: Integration and Coordination. Hierzu dient etwa BPEL („Business Process Execution Language"), mit der es möglich ist, Prozesse zu modellieren und aus einzelnen Aufgaben eine komplexe Anwendung entstehen zu lassen.

Essentiell sind bei Web Services immer Transaktionseigenschaften. Sie können mit geeigneten Spezifikationen beschrieben werden. Solche zusätzlichen Eigenschaften finden sich im Web Service Stack flankierend in einer vertikalen Metadaten-Komponenten wieder. Auf der Seite gegenüber fasst eine Quality-of-Service-Komponente die bisherigen Schichten ein. Den Abschluss der Schichten bilden die Enterprise- oder Grid-Komponenten, auf die hier aus Platzgründen nicht weiter eingegangen wird.

3.2.6 Architektur: Nachrichten-, Service-, Ressourcen-, Richtlinien-Modell

In der W3C-Spezifikation werden Web Services aus unterschiedlichen Perspektiven beschrieben: Einem Policy Model, einem Resource Oriented Model, einem Message Oriented Model und einem Service Oriented Model. Die Grafik Architekturmodell 1 zeigt das Message Oriented Model (Web Services Nachrichten).

Mit diesem Modell wird der Aufbau einer Web Services Nachricht festgelegt, dessen Beziehung zu einem Agenten und wie eine Nachricht zugestellt wird. Die Kästen stehen für Konzepte, die über gerichtete Graphen miteinander in Beziehung stehen. Dass SOAP als Nachrichtenformat genutzt wird, ist dabei nicht zwingend vorgeschrieben, allerdings sollte man es tunlichst verwenden.

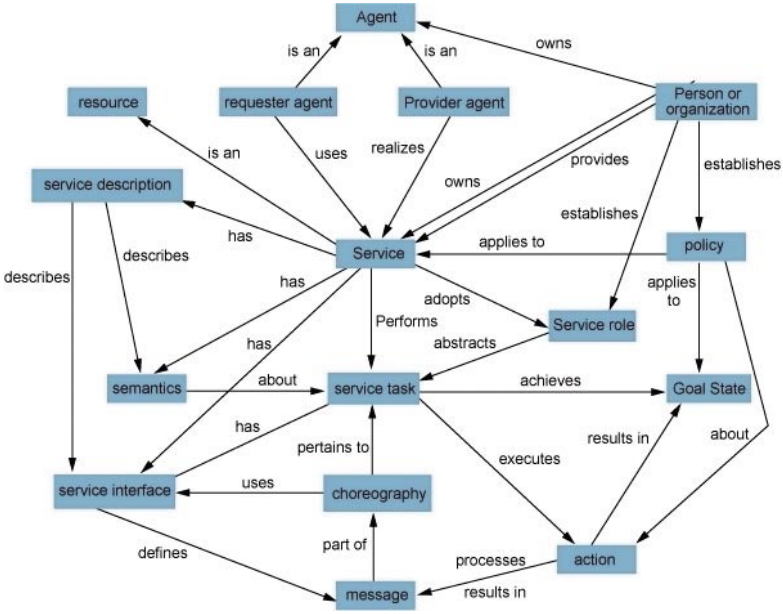


Architekturmodell 1: Der Nachrichtenaufbau von Web Services. (Quelle: Dostal et al: Serviceorientierte Architekturen mit Web Services, Elsevier/Spektrum)

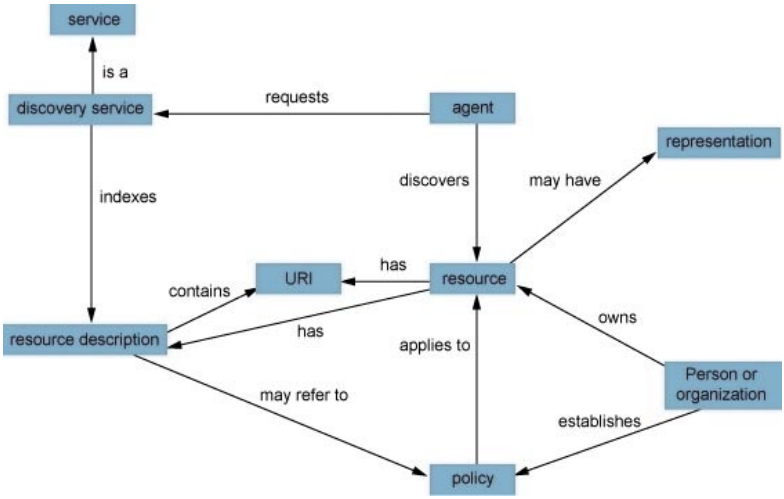
Die Grafik Architekturmodell 2 zeigt das Web Services Modell mit Schwerpunkt Serviceorientierung. Services sind Aktivitäten in einer Web-Services-Architektur. Ein Service wird dabei mit Hilfe eines Agenten realisiert. Beschrieben wird ein Service über ein Service-Interface, wie etwa mit WSDL.

Das Architekturmodell der Ressourcen in der Grafik Architekturmodell 3 beschreibt, wie eine Ressource in einer Web-Services-Architektur definiert ist. Dabei ist eine typische Ressource in der Web-Services-Architektur wiederum ein Web-Service. Mit dem Modell wird festgelegt, dass eine Ressource eindeutig über eine URI („Uniform Resource Identifier“) identifiziert ist. Für einen Web Service, der mit http zu erreichen ist, wäre dies eine URL.

Das letzte Modell ist das Richtlinien- oder Policy-Modell. Es beschreibt den Aufbau von Richtlinien in einer Web-Services-Architektur. Eine Richtlinie ist alles, was Einschränkungen oder Bedingungen definiert. Beispiele für solche Policies sind Sicherheitsaspekte oder Qualitätsmerkmale. Meist werden Policies mit XML-Erweiterungen einem Web-Service hinzugefügt.



Architekturmodell 2: Beispiel eines Dienstes von Web Services. (Quelle: Dostal et al: Service-orientierte Architekturen mit Web Services, Elsevier/Spektrum)



Architekturmodell 3: Ein Ressourcen-Modell von Web Services. (Quelle: Dostal et al: Service-orientierte Architekturen mit Web Services, Elsevier/Spektrum)

3.2.7 Fazit

Web Services sind ihren Kinderschuhen entwachsen. Zahlreiche Unternehmen befassen sich zurzeit mit Web Services und arbeiten an ihrer Verwirklichung. Produktive Ansätze in Form von Standards und Spezifikationen, die gewährleisten, dass die weitere Entwicklung koordiniert weitergeführt wird, wurden bereits geschaffen. Die XML-Basis sorgt für eine starke Integration und hohe Flexibilität.

Dennoch haben Web Services auch mit Problemen zu kämpfen. So leidet das Ansehen darunter, dass es eine schwer überschaubare Anzahl von über Hundert Spezifikationen gibt, die sich zum Teil überlappen und in manchen Fällen auch widersprechen. Unternehmen sehen sich damit der Gefahr ausgesetzt, auf eine falsche Spezifikation zu setzen. Hier heißt es derzeit, Augen offen halten, denn in der aktuellen Situation bilden sich die Spezifikationen heraus, die sich langfristig durchsetzen werden.

Dr. Klaus Manhart

tecCHANNEL-Links zum Thema	Webcode	Compact
Web Services – Grundlagen, Aufbau und Struktur	457051	S.114
Serviceorientierte Architekturen – Grundlegende Konzepte	456248	–
In zehn Schritten zur SOA	569662	–
SOA durch Technik-Angst und mangelndes Wissen gebremst	816629	–
Business Intelligence-Projekte optimal umsetzen	434480	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

3.3 IT-Systeme: Ausfallsicherheit im Kostenvergleich

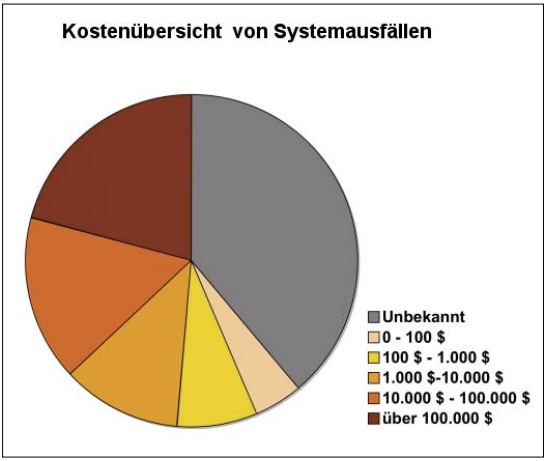
Sicherheit gibt es auch in der IT nicht zum Nulltarif. Wer für seine Geschäftsprozesse mehr Verfügbarkeit benötigt, als sie die handelsüblichen Systeme bieten, muss mit höheren Kosten sowohl in der Anschaffung als auch im Unterhalt rechnen. Allerdings kann der Verzicht auf zusätzliche Sicherheit ganz schön teuer werden – wobei den wenigsten Unternehmen bewusst ist, wie viel sie ein auch nur kurzzeitiger Ausfall ihrer Server-Systeme kosten kann.

Oft besteht schon über die wahrscheinlichen Ausfallzeiten der eingesetzten Systeme nur wenig Klarheit. „Normale“ Server, also Systeme, die nicht speziell für hohe Zuverlässigkeit getunt sind, erreichen heute eine Verfügbarkeit von rund 99,5 Prozent. Das ist zwar erheblich mehr, als solche Geräte früher erreicht haben, bedeutet aber immer noch eine mittlere jährliche Ausfallzeit (Downtime) von über 40 Stunden. Cluster-Systeme erreichen heute Verfügbarkeitswerte zwischen 99,95 und 99,99 Prozent und fallen damit auch noch bis zu einer Stunde pro Jahr aus.

3.3.1 Systemausfälle und ihre Folgen

Die Kosten von einer Stunde Server-Stillstand hängen stark von der jeweiligen Branche und der Art des jeweiligen Geschäftsmodells ab. Auch in Zeiten vollständiger IT-Durchdringung gibt es natürlich immer noch Tätigkeiten, denen man sich zuwenden kann, solange die IT nicht verfügbar ist: Man kann zum Beispiel ein Meeting einberufen, telefonieren, einen Kunden besuchen, eine Kaffeepause halten und die liegengebliebenen Arbeiten später nachholen.

Ausfallkosten: Geschätzte Kosten von Systemausfällen bei HP innerhalb eines Jahres. (Quelle: HP User Group)



Ganz anders verhält es sich, wenn die IT die Prozesse nicht unterstützt, sondern sie unmittelbar steuert. Dann steht während einer Downtime beispielsweise die Produktion oder Auslieferung, Artikel kommen nicht aus dem Lager, Kunden können nicht bestellen oder – noch schlimmer – nicht bezahlen. Die Kosten für ausgefallene Arbeitszeit, als Ergebnis von Stundensatz und Zahl der betroffenen Mitarbeiter, können immer nur einen sehr groben Anhaltspunkt liefern, denn meist sind andere Faktoren gravierender: Womöglich sind auch Vertragsstrafen für nicht rechtzeitig erfolgte Lieferungen zu bezahlen, in der Automobilproduktion heute eine gängige Praxis. Zu den unmittelbaren Ausfallkosten kommen außerdem die schwer zu quantifizierenden Schäden durch Imageverlust wie verärgerte Kunden und Lieferanten.

3.3.2 Die Kosten des Stillstands

Je mehr die Geschäftsprozesse von der IT abhängen, desto seltener werden Fälle, in denen der Stillstand des IT-Systems nur geringfügige Folgen hat. Konnte man zum Beispiel vor zehn Jahren in solchen Fällen wenigstens noch telefonieren, so sind heute auch die Vermittlungsstellen in die IT integriert, zugleich hat sich ein Teil der Kommunikation mit E-Mail direkt auf die IT verlagert.

Anfallende Kosten für Downtime	
Branche	**Kosten pro Stunde (US-Dollar)**
Fertigung	28.000
Logistik	90.000
Einzelhandel	90.000
Home-Shopping	113.000
Medien (Pay per View)	1.100.000
Bankrechenzentrum	2.500.000
Kreditkartenverarbeitung	2.600.000
Broker	6.500.000

(Quelle: Contingency Research)

In Branchen, in denen das ganze Geschäftsmodell von der IT abhängt, können die Downtime-Kosten enorm hoch werden. So schätzt Contingency Research beispielsweise die Ausfallkosten für das Online-Shopping auf über 100.000 Dollar, für ein Bankrechenzentrum auf 2,5 Millionen Dollar und für das Online-Broking gar auf 6,5 Millionen Dollar – pro Stunde Downtime! Auch wenn die Systeme schnell wieder anlaufen, wäre der Schaden gewaltig, denn schon zehn Minuten Stillstand würden den Online-Broker mehr als eine Million kosten.

3.3.3 Systemausfall – das unterschätzte Risiko

Wie hoch die Downtime-Kosten tatsächlich sind, hängt natürlich stark davon ab, wie im Einzelfall die Geschäftsprozesse organisiert sind. Umso bemerkenswerter ist, dass viele Unternehmen die Kosten, die ihnen dabei entstehen, selbst gar nicht kennen. Dies gaben jedenfalls in einer amerikanischen Untersuchung 39 Prozent der befragten IT-Verantwortlichen zu. Wer sich darüber schon Gedanken gemacht hatte, kam teilweise auf recht hohe Werte: Rund ein Drittel rechnete mit Kosten von mehr als 10.000 Dollar, 20 Prozent von ihnen sogar mit über 100.000 Dollar pro Stunde Downtime. Nicht weniger bemerkenswert ist jedoch, dass hierzulande nicht einmal eine entsprechende Untersuchung vorgenommen wurde. Viele Unternehmen wollen sich von den Folgen eines Systemausfalls offenbar überraschen lassen – ein Standpunkt, der unter den Vorzeichen der derzeit so intensiv geführten Compliance-Diskussion kaum zukunftsfähig ist.

Nicht überall ist das Risiko eines Systemausfalls eine betriebswirtschaftlich kalkulierbare Angelegenheit. Wo es um Menschenleben geht, etwa in der Flugsicherung, bei Rettungsleitstellen oder im Gesundheitswesen, muss für die Verfügbarkeit das technisch Mögliche um jeden Preis getan werden; dies gilt auch für die Bereiche, wo staatliche Auflagen hochverfügbare Systeme vorschreiben.

3.3.4 Verfügbarkeit auf unterschiedlichem Niveau

Im kommerziellen Einsatz müssen die möglichen Downtime-Kosten den Kosten für hochverfügbare IT-Systeme gegenübergestellt werden. Hochverfügbarkeit war in der Vergangenheit nur durch teure Spezialsysteme, wie zum Beispiel Tandem Himalaya, oder durch proprietäre Lösungen realisierbar. Diese erforderten Investitionen im Millionenbereich und waren im Unterhalt entsprechend teuer. Ihr Einsatz blieb denn auch speziellen Aufgaben vorbehalten und war für kommerzielle Anforderungen meist nicht wirtschaftlich.

Seit Ende der 90er Jahre sind aber auch verstärkt preiswertere Lösungen verfügbar. Sie verwenden verschiedene Technologien, bieten dementsprechend Verfügbarkeit auf unterschiedlichem Niveau und differieren hinsichtlich der Kosten.

Standby-Systeme: Redundante Systeme übernehmen bei Ausfällen wechselseitig die Prozesse. Durch Umschalten und Übergabe der Prozesse sind Ausfallzeiten unvermeidlich, die Konsistenz von Daten und Transaktionen muss separat sichergestellt werden. Erreichbare Verfügbarkeit: 99,5 bis 99,9 Prozent. Das entspricht einer ungeplanten Downtime von bis zu 8,7 Stunden pro Jahr.

Cluster-Systeme: Wichtige Komponenten der Systeme sind redundant ausgelegt. Bei Störungen sorgen spezielle Algorithmen Software-gesteuert für ein Umschalten, dadurch kommt es zu kurzen Ausfallzeiten beziehungsweise zum Verlust offener Transaktionen. Erreichbare Verfügbarkeit: 99,95 bis 99,99 Prozent. Das entspricht bis zu vier Stunden ungeplanter Downtime pro Jahr.

Fehlertolerante Systeme: Sämtliche Komponenten sind redundant ausgelegt, und alle Prozesse laufen parallel, so dass im Störungsfall keine Zeit durch den Wechsel auf funktionierende Komponenten verloren geht. Erreichbare Verfügbarkeit: 99,999 bis 99,9999 Prozent beziehungsweise maximal fünf Minuten ungeplante Downtime pro Jahr.

Durchschnittliche Ausfallzeiten in Abhängigkeit vom Verfügbarkeitsniveau (in Stunden)			
Verfügbarkeit (Prozent)	**Betriebszeiten 7 x 24 Stunden**	**Betriebszeiten 7 x 12 Stunden**	**Betriebszeiten 5 x 12 Stunden**
Betriebsstunden pro Jahr	8760	4380	3132
99,00000	87,6000	43,8000	31,3200
99,50000	43,8000	21,9000	15,6600
99,90000	8,7600	4,3800	3,1320
99,95000	4,3800	2,1900	1,5660
99,99000	0,8760	0,4380	0,3132
99,99500	0,4380	0,2190	0,1566
99,99900	0,0876	0,0438	0,0313
99,99990	0,0088	0,0044	0,0031
99,99999	0,0009	0,0004	0,0003

3.3.5 Ausfallsichere Systeme im Kostenvergleich

Auf der Kostenseite sind neben der Beschaffung der Hardware natürlich eine Reihe weiterer Faktoren zu berücksichtigen, so insbesondere die Kosten von Betriebssystem, Datenbanken, Applikationen, Implementierung, Serviceverträgen, Schulungen sowie die Betriebskosten für Administration und so weiter. Entsprechend der technologischen Eigenarten der genannten Systeme schlagen diese Faktoren verschieden zu Buche.

So müssen Applikationen für Cluster-Systeme angepasst werden, damit sie deren Leistungsfähigkeit auch in vollem Umfang nutzen können. Demgegenüber sind Standby-Server mit normaler Software zufrieden. Fehlertolerante Systeme sind seit einiger Zeit auch für die Standard-Betriebssysteme Windows und Linux verfügbar, die entsprechenden Applikationen laufen ohne Änderungen. Insbesondere ist die Implementierung eines Cluster-Systems viel aufwendiger als die eines fehlertoleranten Servers. Dieser ist zwar intern redundant ausgelegt, was für den Anwender jedoch völlig transparent ist – ihm gegenüber präsentiert sich der fehlertolerante Server wie ein Stand-alone-Gerät.

Kostenaufschlüsselung ausfallsicherer Systeme (in Euro)			
Komponentenkosten	**Standby**	**Cluster**	**Fehlertoleranter Server**
Hardware	8.000	11.000	33.000
Betriebssystem	5.000	6.000	3.000
Datenbank	10.000	20.000	7.500
Applikation	8.000	8.000	4.000
Implementierung	1.000	9.000	3.000
Test	1.000	10.000	3.000
Schulung	0,00	3.000	0,00
Systemkosten	33.000	67.000	53.500
Laufende Kosten			
Support pro Jahr	1.500	5.000	0,00
Service pro Jahr	1.000	12.000	5.000
Laufende Kosten gesamt	2.500	17.000	5.000

Da ein solches System nicht nur virtuell, sondern auch physikalisch ein einziger Rechner ist, benötigt es anders als Standby- oder Cluster-Server auch nur jeweils eine Softwarelizenz, was beispielsweise bei Datenbanken einen wichtigen Kostenfaktor darstellt. Die auf den ersten Blick höheren Anschaffungskosten der fehlertoleranten Systeme gegenüber den Cluster-Servern gleichen sich so bei Einbeziehung sämtlicher Kostenfaktoren wieder aus. Dazu kommt, dass bei Cluster-Systemen Administration, Service und Support deutlich aufwendiger sind, so dass hier mit hohen laufenden Kosten zu rechnen ist.

Jährliche Gesamtkosten für ausfallsichere Systeme (in Euro)			
Nutzungszeit	**Standby**	**Cluster**	**Fehlertoleranter Server**
1 Jahr	35.500	84.000	58.500
2 Jahre	19.000	50.500	31.750
5 Jahre	9.100	30.400	15.700

3.3.6 Ausfallkosten im Vergleich

Unterm Strich sind die gesamten Anschaffungs- und Betriebskosten für Standby-Systeme am günstigsten. Hier gibt es ja auch keine technisch abgesicherte Verfügbarkeit, durch das bloße Bereithalten eines zweiten Servers wird ein System nicht

hochverfügbar. Fehlertolerante Server erweisen sich bei Berücksichtigung aller Kostenfaktoren erstaunlicherweise schon in der Anschaffung als teurer. Klammert man die besonders kostentreibende Datenbank aus, so liegen diese beiden Alternativen gleichauf, durch die günstigeren laufenden Kosten haben die fehlertoleranten Server, sobald es in den Betrieb geht, die Nase wieder vorn.

Fehlertolerante Systeme im Vergleich (Euro pro Jahr, Nutzungszeit fünf Jahre)			
	Standby	**Cluster**	**Fehlertoleranter Server**
Verfügbarkeit (Prozent)	99,9	99,95	99,999
Systemkosten (zirka Angaben in Euro)	9.100	30.400	15.700
Downtime-Kosten (zirka Angaben in Euro)	180.000	90.000	2.000

Ob eine solche Investition und Kosten unterm Strich sinnvoll sind, zeigt der Vergleich mit den Kosten eines möglichen Systemausfalls. Pauschalisierte Downtime-Kosten, die für einen direkten Vergleich nötig wären, lassen sich aber schwer schätzen, weil sie, wie erwähnt, sehr stark von der Branche und vom jeweiligen Unternehmen abhängen. Verwendet man als Hilfsgröße die Kosten einer Industriestunde pro Mitarbeiter (43,50 Euro) und multipliziert diesen Wert mit der Ausfallwahrscheinlichkeit, so ergeben sich für die drei alternativen Lösungen bei 500 Mitarbeitern und einem 7x24-Stunden-Betrieb folgende hypothetische Szenarien:

Ausfallkosten abhängig von Betriebszeiten und Verfügbarkeitsniveau (in Euro, 500 Mitarbeiter, Kosten 42,50 je Stunde)			
Verfügbarkeit (Prozent)	**Betriebszeiten 7 x 24 Stunden**	**Betriebszeiten 7 x 12 Stunden**	**Betriebszeiten 5 x 12 Stunden**
99,00000	1.861.500	930.750	443.700
99,50000	930.750	465.375	221.850
99,90000	186.150	93.075	44.370
99,95000	93.075	46.538	22.185
99,99000	18.615	9.308	4.437
99,99500	9.308	4.654	2.219
99,99900	1.862	931	444
99,99990	186,15	93,08	44,37
99,99999	18,62	9,31	4,44

3.3.7 Fazit und Ausblick

Die errechneten Kosten eines IT-Ausfalls können allerdings nur eine grobe Orientierung hinsichtlich der Dimensionen geben, in denen sich das Restrisiko eines Unternehmens bewegt. Im Einzelfall, wenn durch einen Systemausfall beispielsweise Kundenbeziehungen auf dem Spiel stehen oder gar die Existenz eines Unternehmens bedroht ist, können die Kosten weit höher liegen.

Spätestens dann erweisen sich vermeintlich preiswerte Lösungen wie Standby-Systeme als äußerst kostspielig. Aber auch Cluster-Systeme besitzen Schwachstellen. Eine Alternative können entsprechend konfigurierte und dimensionierte fehlertolerante Server-Systeme sein. Sie verwenden preiswerte Standardtechnologien und können in unterschiedlichen Anwendungsgebieten eingesetzt werden.

Ulrich Lenz

tecCHANNEL-Links zum Thema	Webcode	Compact
IT-Systeme: Ausfallsicherheit im Kostenvergleich	458076	S.125
IT-Sicherheit: Neue Pflichten für das Management	431240	–
Von der Pflicht zur Kür: Sicherheit als Prozess aufsetzen	445112	–
Patch-Management: Mehr Lücken, immer weniger Zeit	449803	–
Hochverfügbarkeit: Cluster contra Server	456463	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

3.4 Oracle Datenbank-Tuning

Die Leistungsfähigkeit einer Datenbank hängt vor allem davon ab, wie gut sie auf die speziellen Bedürfnisse angepasst ist. Eine Standard-Installation kann den besonderen Anforderungen einer Anwendung nur selten gerecht werden. An welchen Stellschrauben Sie bei Oracle drehen können, zeigt unsere neue Serie.

Datenbanken sind das Herz vieler Business-Applikationen oder Websites. Der Erfolg steht und fällt mit der Geschwindigkeit, in die Datenbank Anfragen bearbeitet. Kommt die Antwort auf eine Web-Anfrage zu spät, könnte der Besucher schon wieder verschwunden sein und anderswo bestellen. In diesem Teil unserer Serie gehen wir auf grundlegende Fakten ein, die die Performance einer Datenbank beeinflussen, und auf die zur Verfügung stehenden Statistik-Tools, die bei der Fehlersuche behilflich sind. Die weiteren Teile der Oracle-Serie finden Sie online auf tecCHANNEL (**Webcode 455264** und **456311**).

3.4.1 Datenbank Tuning

Oracle plant seit längerem, das Umfeld für eine sich selbst verwaltende Datenbank zu schaffen. Während man in Oracle9i mit der Einführung von dynamischen Parametern für die Shared Memory-Verwaltung nur von ersten Ansätzen sprechen konnte, finden sich in Oracle 10g die ersten Features, die ein automatisches Tuning in Abhängigkeit vom aktuellen Workload, ohne Eingriff durch den DBA, durchführen. Es ist zu erwarten, dass Oracle diesen Weg konsequent weitergeht. Automatisches Tuning oder eine sich selbst verwaltende Datenbank bietet Vorzüge in mehreren Bereichen:

- Die Datenbankparameter können dynamisch, abhängig vom aktuellen Workload der Datenbank, angepasst werden. Dagegen ist eine statische Konfiguration immer ein Kompromiss, der alle Situationen über die Zeitachse gleichermaßen bedienen muss.
- Mit dem Einstieg in die Welt des Grid Computing ist ein Service Provisioning auf allen Ebenen erforderlich.
- Für kleine und mittlere Datenbanken nimmt der Anteil der Einflussnahme durch den Datenbankadministrator ab. Das macht die Oracle-Datenbank konkurrenzfähiger gegenüber Datenbanken wie Sybase oder Informix.

Bei genauer Betrachtung lässt sich jedoch sagen, dass generell der Administrationsaufwand einer Oracle 10g-Datenbank gegenüber früheren Versionen nicht kleiner geworden ist. Die Einsparungen an Administration durch automatische Features und Vereinfachungen werden durch die große Anzahl neuer Produkte und Features kompensiert. Es erfolgt also eine Verlagerung der Charakteristik der administrativen Aufgaben.

Wenn wir über Oracle 10g-Datenbank-Tuning sprechen, dann lassen sich die Aktivitäten in folgende Kategorien einteilen:

- Performance-Planung
- Optimierung von Instanz und Datenbank
- Einrichtung automatischer Tuning-Features

3.4.2 Performance-Planung

Performance-Planung bekommt einen immer größeren Einfluss auf die Leistungsfähigkeit des Endsystems. Vor wenigen Jahren war die Standardvorgehensweise noch, eine Datenbank aufzusetzen und danach schrittweise zu optimieren. Dieses Vorgehen ist heute nicht mehr ausreichend. Bereits bei Festlegung der Architektur kann durch falsche Entscheidungen die Leistungsfähigkeit des Systems stark eingeschränkt werden. Das lässt sich auch später durch Tuning-Maßnahmen oder durch Einsatz leistungsstärkerer Hardware nicht in vollem Umfang korrigieren. So bringt der Einsatz einer Real Application Clusters-Architektur nicht nur eine Erhöhung der Verfügbarkeit, sondern auch eine nicht unerhebliche Verbesserung an Performance.

So hat in einem Projekt die Verfügbarkeit bei der Auswahl einer RAC-Architektur eine untergeordnete Rolle gespielt. Es sollte ein Advanced Queuing-System zum Einsatz kommen, bei dem eine Durchsatzrate von zweitausend Nachrichten pro Sekunde erforderlich war. Oracle Advanced Queuing speichert alle Nachrichten in der Datenbank. Die Flaschenhälse bilden dabei die Online Redo Log-Dateien sowie die Undo-Tablespaces. Da in einer RAC-Architektur jede Instanz über eigene Redo Log-Dateien und Undo-Tablespaces verfügt, konnte ein Skalierungsfaktor von 0,8 erreicht werden. Das heißt, mit zwei Instanzen konnte der Durchsatz auf 180%, bei vier Instanzen auf ca. 320% erhöht werden.

Skalierbarkeit

Skalierbarkeit spielt häufig im Internetbereich die erste Geige. Es ist fast unmöglich einzuschätzen, wie sich die Zugriffszahlen entwickeln werden. Auch hier kann einfach durch Hinzunahme weiterer Knoten eine Erhöhung der Performance erfolgen. Dabei ist keine Änderung in der Applikation erforderlich. Bekanntlich machen die Applikationskosten den Löwenanteil von Internetprojekten aus. RAC bietet in diesem Fall die perfekte Kombination aus einem hohen Maß an Skalierbarkeit und Hochverfügbarkeit.

Es gibt weitere Optionen, um Performance bereits bei der Architekturerstellung zu planen. So können Sie sich für eine logische Standby-Datenbank entscheiden, die mit Oracle Streams aktuell gehalten wird. Alle Benutzerabfragen und Reports können dann auf die Standby-Datenbank umgeleitet werden. Zusätzlich können Sie die Primär-Datenbank für DML-Befehle und die Standby-Datenbank für SQL-Abfragen optimieren. Das Maß an Entlastung, das Sie auf der Primär-Datenbank

damit erreichen, erhalten Sie selten durch den Einsatz leistungsfähigerer Hardware. Zudem ist die letztere Methode wesentlich teurer.

> Führen Sie vor der endgültigen Architektur-Entscheidung einen Proof-of-Concept-Test durch. Damit können Sie u.a. beweisen, dass die vorgeschlagene Architektur die erforderlichen Performance-Werte liefert. Dabei ist immer noch Raum für spätere Tuning-Aktivitäten.

Auswahl der Hardware-Komponenten

Zur Performance-Planung gehört auch die richtige Auswahl und die Dimensionierung der Hardware-Komponenten. Wenn Sie ein ausfallsicheres System benötigen, dann werden Sie von vornherein Festplatten oder Subsysteme spiegeln oder evtl. ein RAID-System einsetzen wollen.

Für eine Data Warehouse-Datenbank stehen andere Aspekte im Vordergrund. Hier kommt es fast in erster Linie auf Performance an, alle anderen Aspekte treten in den Hintergrund. Auch Verfügbarkeit spielt eher eine untergeordnete Rolle. Es werden riesige Datenmengen verarbeitet, die nur schwer in den Buffer Cache passen. Besonderer Wert sollte deshalb auf hohe Durchsatzraten für E/A-Vorgänge gelegt werden. Hier macht es also wenig Sinn, Festplatten zu spiegeln oder RAID-5-Systeme einzusetzen.

Das Datenbank-Modell hat ebenfalls einen wichtigen Einfluss auf die Performance des produktiven Systems. In der Praxis zeigt sich, dass logisch perfekte Modelle nicht immer die beste Performance liefern. Verwenden Sie z.B. hierarchische Tabellen, die sehr groß sind, dann laufen die Abfragen sehr lang und haben einen großen Ressourcen-Verbrauch. Ein Modell ohne Redundanzen ist zwar erstrebenswert, jedoch kann ein gewisses Maß von Datenredundanz eine deutliche Erhöhung der Performance zur Folge haben. Nicht umsonst ist ein Data Warehouse mit einem Star-Schema ein hochredundantes System.

> Formulieren Sie, bevor Sie mit der Performance-Planung beginnen, eindeutige Zielsetzungen. Systeme können sehr unterschiedliche Prioritäten aufweisen. So kann einerseits die Laufzeit der Applikation, anderseits eine optimale Strukturierung der Daten im Vordergrund stehen. Erfüllen Sie nur die Mindestanforderungen an die Performance und versuchen Sie nicht, die optimale Performance auf Kosten von Nachteilen in anderen Bereichen herauszuholen. In der Zielsetzung sollten auch Anforderungen an die Skalierbarkeit enthalten sein. Hochskalierbare Systeme sind in der Regel teurer und erfordern eine komplexere Architektur.

3.4.3 Optimierung von Instanz und Datenbank

Oracle hat mit der Version 10g begonnen, automatische Tuning-Features auszuliefern. Damit ist es möglich, über die Zeitachse Datenbankparameter abhängig vom aktuellen Workload dynamisch zu verändern. Ausführliche Informationen dazu finden Sie im Artikel Oracle Datenbank-Tuning Teil 3 im Abschnitt „Einrichtung automatischer Tuning-Features“ (**Webcode 456311**).

Der vorliegende Abschnitt beschäftigt sich mit der Optimierung eines statischen Systems, bei dem sich die Parameter und Rahmenbedingungen über die Zeitachse nicht verändern. Der Datenbankadministrator sammelt Statistiken, um die Performance-Probleme zu lokalisieren und zu analysieren. Danach unternimmt er Schritte, um die Performance zu verbessern. Dabei werden Parameter angepasst und bleiben wieder konstant bis zum nächsten Tuning.

Sammeln Sie Ihre ersten Tuning-Erfahrungen mit statischen Systemen. Die Kenntnis der Auswirkungen von Initialisierungsparametern sowie Erfahrungen zum effektiven Vorgehen bei der Lösung von Performanceproblemen sind Grundvoraussetzung für einen erfolgreichen Tuning-Prozess. Automatische Tuning-Features lösen bei weitem nicht alle Performance-Probleme. Hier sind manuelle Eingriffe ebenso erforderlich, mit dem zusätzlichen Faktor von dynamischen Zuständen des Datenbanksystems.

3.4.4 Eine performante Datenbank erstellen

Datenbank-Tuning beginnt mit der Ersterstellung einer Datenbank und ihrer Objekte. Bereits hier können Sie durch Abweichung von der Standardkonfiguration erste Performance-Verbesserungen erreichen.

Physische Objekte

In Oracle 10g haben Sie die Möglichkeit, mehrere Temporary Tablespaces zu einer Gruppe zusammenzufassen. Damit kann eine SQL-Anweisung mehrere Tablespaces gleichzeitig benutzen. Wenn in Ihrem System viele Sortierprozesse laufen, können Sie mit Hilfe von Gruppen für Temporary Tablespaces eine Performance-Verbesserung erreichen.

Die Größe der Online Redo Log-Dateien hat Einfluss auf die Performance der Datenbank. Das Verhalten des Log-Writer-Prozesses (DBW*n*) hängt von deren Größe ab. In der Regel garantieren große Redo Log-Dateien eine verbesserte Performance. Kleine Dateien vergrößern dagegen die Checkpoint-Häufigkeit. Es gibt keine allgemeinverbindliche Regel, wie groß die Redo Log-Dateien sein sollen, aber Größen von mehreren hundert Megabyte bis in den Gigabyte-Bereich hinein sind durchaus keine Seltenheit mehr. Ein Wechsel der Log-Datei alle zwanzig Minuten ist ein guter Anhaltspunkt.

Segmente

Beim Erstellen einer Tabelle reserviert Oracle Speicherplatz in Form eines Extents. Wächst die Tabelle durch Einfügen von Daten, werden weitere Extents hinzugenommen. Besteht ein Segment aus vielen kleinen Extents, die unter Umständen noch wahllos über die Festplatte verteilt sind, dann nennt man diese Situation Fragmentierung. Ein stark fragmentiertes Segment führt zu einer signifikanten Verschlechterung der Performance. Handelt es sich dabei um eine häufig frequentierte Tabelle, kann es zu Wartezeiten von mehreren Minuten kommen. Tablespaces, in denen der Administrator die Verwaltung der Segmente bestimmt, werden „Vom Datenbankkatalog verwaltete Tablespaces" genannt, da die Größe und Anzahl von Extents im Datenbankkatalog hinterlegt werden. Lokal verwaltete Tablespaces gibt es seit Oracle8i. Dabei übernimmt Oracle die Verwaltung der Extents in Form von Bitmaps und Sie haben nur wenig Einflussnahme.

> Verwenden Sie in Oracle 10g für kleine bis große Segmente lokal verwaltete Tablespaces. Das vermindert den Verwaltungsaufwand und bringt keine Nachteile für die Performance mit sich. Für sehr große Segmente kann es Sinn machen, vom Datenbankkatalog verwaltete Tablespaces zu verwenden. Wenn Sie große lokal verwaltete Tablespaces erstellen, dann sollten Sie eine gleichförmige Extent-Zuweisung verwenden.

Der effizienteste Weg, Indexe zu erstellen, ist, zuerst die Daten in die Tabelle zu laden, ohne dass ein Index angelegt ist, und hinterher die Indexe zu erstellen. Auch beim Erstellen der Indexe lässt sich viel Zeit sparen. Entscheidend für die Geschwindigkeit beim Indexaufbau ist die Sort Area. Eine Erhöhung des Parameters `SORT_AREA_SIZE` vergrößert die Sort Area und Oracle führt bei der Erstellung des Index weniger Zugriffe auf die Festplatte durch. Ein Index kann mit der Option `UNRECOVERABLE` erstellt werden. In diesem Fall werden wesentlich weniger Redo-Informationen erzeugt.

Hauptspeicher-Verwaltung

Oracle speichert Informationen im Hauptspeicher, um Plattenzugriffe zu reduzieren. Das Ziel ist deshalb, die Anzahl der Festplattenzugriffe so gering wie möglich zu halten und die Informationen im Hauptspeicher verfügbar zu machen. Seit Oracle9i ist es möglich, die Größen für den Shared Pool, den Large Pool und den Buffer Cache dynamisch, d.h. ohne Neustart der Instanz, zu verändern.

> Achten Sie darauf, dass die System Global Area (SGA) komplett im realen Hauptspeicher läuft. Eine Benutzung der Swap-Datei führt zu großen Performanceverlusten und verfälscht die Bilder, die Sie von den Statistiken erhalten. Problemlösungen sind eine Verkleinerung der SGA oder eine Erhöhung der realen Hauptspeichergröße.

Der Parameter LOCK_SGA kann auf einigen Plattformen benutzt werden, um die SGA im realen Hauptspeicher festzubinden. Damit wird ein Schreiben in die Auslagerungsdatei vermieden.

Wie groß die einzelnen Pools zu wählen sind, hängt von Last und Größe der Datenbank sowie von der Art der Anwendung und SQL-Anweisungen ab. Generell gilt die Aussage: Je größer, desto besser. Da aber der reale Speicher begrenzt ist, macht es keinen Sinn, Speicher einerseits zu verschenken, wenn er an anderer Stelle benötigt wird.

Festplatten-Aktivitäten

Die Architektur einer Oracle-Datenbank garantiert, dass Performance nicht durch Wartezeiten auf Ein- und Ausgabeaktivitäten der Festplatte eingeschränkt wird. Allerdings wird in der Praxis ein intelligentes E/A-Layout vorausgesetzt. Bei einem schlechten E/A-Layout kann es zu großen Verlusten an Performance kommen. Eine gute E/A-Performance beginnt deshalb bereits bei der Auswahl der Hardware. Der Durchsatz in Megabyte pro Sekunde ist eine wichtige Größe.

Ein intelligentes Verteilen von Dateien auf verschiedene Festplatten (Striping) trägt entscheidend zur Erhöhung des E/A-Durchsatzes bei. Es gibt verschiedene Formen des Stripings. Weit verbreitet ist die Methode, große und häufig benutzte Tablespaces auf mehrere Dateien aufzuteilen und diese auf verschiedene Festplatten zu verteilen. Dann sind mehrere Festplatten parallel mit dem Lesen beschäftigt.

Die Art der Verteilung von Dateien hängt stark vom Einsatzgebiet ab. Während in einer OLTP-Datenbank die Online Redo Log-Dateien stark beschäftigt sind und deshalb unbedingt separiert werden müssen, werden sie im Data Warehouse von SQL-Abfragen nicht benutzt. Auch bei einem sehr guten Anfangslayout werden Sie im laufenden Betrieb feststellen, dass die Verteilung noch nicht optimal ist. Eine Überwachung der E/A-Aktivitäten ist deshalb wichtig. Hot Spots können identifiziert und beseitigt werden.

Verwaltung von Festplatten-Subsystemen

Es werden immer häufiger Festplatten-Subsysteme eingesetzt, die über SAN oder NAS angeschlossen werden. Die Verwaltung und die Zuweisung erfolgt dann über Logical Volume Manager. Auch hier gibt es eine Möglichkeit zur Einflussnahme auf die Verteilung von Dateien. So können Dateien über verschiedene Disk-Gruppen verteilt werden und liegen dann auch physisch getrennt.

Auch die richtige Wahl der Blockgröße trägt zur Verbesserung der Performance bei. Während in einem Data Warehouse höhere Blockgrößen Verbesserungen erzielen, kann im OLTP-System ein Gegeneffekt eintreten. Im Folgenden finden Sie Regeln, die Ihnen helfen, die richtige Blockgröße für Ihr System zu bestimmen.

Für Lesezugriffe gilt:

- Für kurze Sätze und überwiegend zufällige Lesezugriffe sind kleinere Blockgrößen besser.
- Sind die Sätze kurz und wird überwiegend sequenziell zugegriffen, dann sind größere Blöcke besser.
- Wenn die Sätze sehr lang sind und LOBs in großer Anzahl enthalten, dann sind größere Blöcke zu bevorzugen.

Für Schreibzugriffe gilt:

- Für OLTP-Datenbanken mit vielen Transaktionen sollte die Blockgröße nicht zu groß gewählt werden. Im Falle eines Kompromisses ist der kleinere Wert zu bevorzugen.
- Für ein Data Warehouse sollten eher große Blöcke verwendet werden, auch wenn das zu einer Verlangsamung im Ladeprozess führt.
- Wenn Sie sich nicht sicher sind, welche Blockgröße Sie wählen sollen, dann ist 8 Kbyte ein guter Kompromiss, der eventuell nicht optimal ist, aber andererseits auch keine Probleme verursacht.

Crash Recovery

Oracle führt ein Crash Recovery durch, wenn sich die Datenbank in einem inkonsistenten Zustand befindet. Das ist z.B. der Fall bei einem Neustart nach einem `shutdown abort`. Die Zeit für ein Crash Recovery kann sehr lang sein, wenn der letzte Checkpoint lange zurückliegt. Zu häufige Checkpoints andererseits führen zu einer Verschlechterung der Performance. An dieser Stelle ist also ein Kompromiss zu finden. Mit dem Parameter `fast_start_mttr_target` ist es möglich, die Recovery-Zeit zu steuern.

Statistiken sammeln

Das Sammeln von Statistiken ist die Basis für ein erfolgreiches Performance-Tuning. Nur mit Hilfe der Statistiken können Sie sich ein komplettes Bild über die Aktivitäten in der Datenbank machen. Sie können kritische Ereignisse und Engpässe erkennen und gezielt Statistiken abfragen.

> Sammeln Sie Statistiken über längere Zeiträume. Archivieren Sie ältere Statistiken, aber löschen Sie diese nicht. Nur mit einer kompletten Historie sind Sie in der Lage, die richtigen Schlüsse über das System zu ziehen.

Oracle stellt die folgenden Mittel zum Sammeln von Statistiken zur Verfügung:

- das Automatic Workload Repository (AWR)
- die v$-Views im Datenbankkatalog

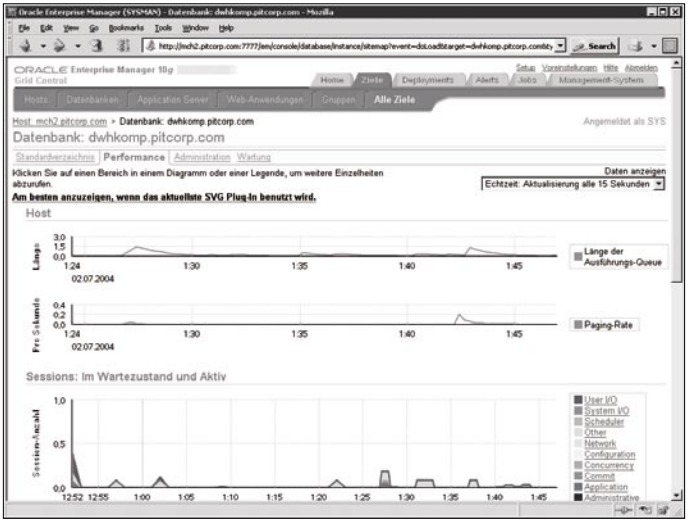
Sie können die gesammelten Informationen des AWR für die Datenbank-Optimierung verwenden. Das Einführen des AWR dient in erster Linie der Verwendung durch die automatischen Tuning Features. Das Automatic Workload Repository wurde auf Basis von STATSPACK weiterentwickelt und löst STATSPACK ab.

> Beachten Sie, dass beim Herunterfahren einer Instanz die Statistiken in den V$-Views gelöscht werden. Wenn Sie also Statistiken über einen längeren Zeitraum sammeln wollen, reichen die V$-Views alleine nicht aus.

Enterprise Manager

Der Enterprise Manager bietet Momentaufnahmen für Performance-Werte. Klicken Sie zur Anzeige auf das Register PERFORMANCE der Datenbank-Seite. Die V$-Views sind die Basis für alle Werkzeuge zum Sammeln und Anzeigen von Statistiken. Sie können darauf aufbauend Ihre eigenen Performance-Werkzeuge erstellen. Allerdings decken die vorhandenen Tools die Statistiken ab, die Sie in der Praxis benötigen.

> Als Administrator sollten Sie die wichtigsten Views kennen. Nicht immer stehen bei Kunden ad hoc die entsprechenden Werkzeuge zur Verfügung. Dann können Sie notwendige Informationen über SQL*Plus abfragen.



Enterprise Manager: Performance Übersicht

Die V$-Views lassen sich in drei Kategorien einteilen:

- Current State Views
- Counter/Accumulator Views
- Information Views

Current State Views

Current State Views spiegeln den aktuellen Zustand in der Datenbank wider. In folgender Tabelle finden Sie eine Übersicht.

Current State Views	
View	**Beschreibung**
V$LOCK	Locks, die momentan gehalten oder angefordert werden
V$LATCHHOLDER	Sitzungen und Prozesse, die ein Latch aufweisen
V$OPEN_CURSOR	Alle in der Instanz offenen Cursor
V$SESSION	Alle offenen Sitzungen
V$SESSION_WAIT	Ressourcen, auf die momentan gewartet wird

Counter/Accumulater Views

Counter/Accumulater Views speichern, wie oft bestimmte Aktivitäten seit dem Start der Instanz stattgefunden haben.

Counter/Accumulator-Views	
View	**Beschreibung**
V$DB_OBJECT_CACHE	Statistik des Shared Pools auf Objekt-Niveau
V$FILESTAT	E/A-Aktivitäten auf Datei-Niveau
V$LATCH	Zusammenfassung von Latch-Aktivitäten
V$LATCH_CHILDREN	Aktivitäten von Child Latches
V$LIBRARY_CACHE	Statistik für den Shared Pool auf Namespace-Niveau
V$LIBRARY_CACHE_MEMORY	Zusammenfassung über die Benutzung des Library Cache

V$MYSTAT	Zusammenfassung über die Benutzung von Ressourcen der eigenen Sitzung
V$ROLLSTAT	Zusammenfassung der Aktivität von Rollbacksegmenten
V$ROWCACHE	Zusammenfassung der Aktivitäten des Dictionary Cache
V$SEGMENT_STATISTICS	Überwachung der Segment-Statistik
V$SEGSTAT	Realzeit-Überwachung von Segmenten
V$SESSION_EVENT	Zusammenfassung der Warte-Ereignisse in der aktuellen Sitzung
V$SESSTAT	Ressourcen-Benutzung, seit die Sitzung existiert
V$LIBRARY_CACHE_MEMORY	Simulation des LRU-Mechanismus im Shared Pool
V$SQL	Detailinformationen für Cursor von V$SQLAREA
V$SQLAREA	SQL-Befehle im Shared Pool
V$SYSSTAT	Zusammenfassung der Benutzung von Ressourcen
V$SYSTEM_EVENT	Zusammenfassung von Ressourcen, auf die gewartet wurde
V$UNDOSTAT	Historie der Benutzung von UNDO im Zehn-Minuten-Takt
V$WAITSTAT	Buffer Waits pro Block

Information Views

Information Views sind weniger dynamisch als Current State Views.

Information Views	
View	**Beschreibung**
V$MTTR_TARGET_ADVICE	Empfehlungen des MTTR Advisors, wenn der Parameter fast_start_mttr_target gesetzt ist
V$PARAMETER V$SYSTEM_PARAMETER	Parameter der aktuellen Sitzung und Instanz-Parameter
V$PROCESS	Server-Prozesse
V$SEGSTAT_NAME	Segment-Statistik

V$SQL_PLAN	Ausführungsplan des letzten Cursors
V$SQL_PLAN_STATISTICS	Details für den Ausführungsplan
V$SQL_TEXT	Text der SQL-Anweisungen im Shared Pool

Sonstige Views

Oracle 10g stellt Performance-Views zur Verfügung, die sich auf das Automatic Storage Management beziehen.

Views für das Automatic Storage Management	
View	**Beschreibung**
V$ASM_DISKGROUP	Beschreibung der Diskgroups einer ASM-Instanz (Nummer, Name, Größe, Status, Redundanz-Typ). In einer DB-Instanz eine Zeile für jede Diskgroup, die verwendet wird.
V$ASM_CLIENT	Anzeige der Datenbanken, die diese Diskgroups benutzen. In einer DB-Instanz eine Zeile für die ASM-Instanz, die verwendet wird
V$ASM_DISK	Verfügbare Platten. In einer DB-Instanz eine Zeile für jede Platte, die von dieser Instanz verwendet wird.
V$ASM_FILE	In der ASM-Instanz die Dateien, die zu einer Diskgroup gehören. In einer DB-Instanz keine Zeilen.
V$ASM_TEMPLATE	In der ASM-Instanz das Template für eine gemountete Diskgroup. In einer DB-Instanz keine Zeilen.
V$ASM_ALIAS	In der ASM-Instanz die Alias-Namen der Diskgroups. In einer DB-Instanz keine Zeilen.
V$ASM_OPERATION	In der ASM-Instanz die Anzeige von laufenden Operationen. In einer DB-Instanz keine Zeilen.

Neu in Oracle 10g sind Views für das verbesserte Wait-Event-Modell.

Neue V$-Views für das Wait-Event-Modell	
View	**Beschreibung**
V$SYSTEM_WAIT_CLASS	Liefert Zeiten für Warte-Ereignisse sowie die in jeder Klasse verbrauchte Zeit für die gesamte Instanz
V$SESSION_WAIT_CLASS	Speichert die Anzahl von Warte-Ereignissen auf Sitzungsbasis
V$SESSION_WAIT_HISTORY	Zeigt die letzten zehn Warte-Ereignisse für alle aktiven Sitzungen an
V$EVENT_HISTOGRAMM	Für die Darstellung eines Histogramms der Anzahl der Ereignisse sowie der maximalen und Gesamt-Wartezeit
V$FILE_HISTOGRAMM	Stellt ein Histogramm aller einzelnen Block-Lesevorgänge dar. Die Darstellung erfolgt pro Datei.
V$TEMP_HISTOGRAMM	Liefert ein Histogramm aller Block-Lesevorgänge pro temporärer Datei

In einer Real-Application-Clusters-Datenbank existieren Views mit dem Präfix GV$. Diese enthalten eine Spalte mit der Instanznummer und führen eine datenbankübergreifende Statistik.

Ulrich Lenz

Weiterführende Infos

Unsere Artikel zu Oracle 10g basiert auf Kapitel 18 des Standardwerks „Oracle 10g“ von Fröhlich, Czarski und Maier aus dem Verlag Markt + Technik. Sie können dieses über 870 Seiten starke Buch auch in unserem Buchshop (www.tecchannel.de) bestellen oder als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Oracle Datenbank-Tuning	453121	S.132
Der Shared Pool	455264	–
Buffer Cache optimieren	456311	–

4. Windows Server / Exchange Inside

Beim Sicherheitsmanagement von Netzenwerken auf Basis von Windows Server und Exchange stecken die Tücken oft im Detail. Etwa wenn es um die Abwehr von Spam und Malware geht. Knifflig ist auch der Umgang mit Gruppenrichtlinien. Sowohl allgemeine Systemeinstellungen als auch Sicherheitsparameter lassen sich darüber zentral vorgeben. Die wichtigste Maßnahme für mehr Sicherheit im Active Directory ist die gezielte Vergabe von Zugriffsberechtigungen.

4.1 Spam- und Virenabwehr mit Exchange

Unerwünschte E-Mails und darin enthaltene Viren führen zu einer gravierenden Belastung jedes E-Mail-Empfängers. Eine unaufhaltsame Flut von Würmern und Angeboten für Pillen, Pornographie und Persönlichkeitsentwicklung ergießt sich aus dem Internet über Ihre Exchange-Server. Solange sich Berge von Müll, gefährlichem Müll, im Posteingang anhäufen, werden Sie die Benutzer nicht von der Qualität Ihrer Arbeit als Administrator überzeugen können.

4.4.1 So gelangen Spammer an Ihre Adresse

Spammer sammeln E-Mail-Adressen aus den unterschiedlichsten Quellen. Am beliebtesten sind Usenet-Newsgroups und die Websites Ihrer Organisation. Weisen Sie die Benutzer und Webentwickler darauf hin, dass E-Mail-Adressen immer unkenntlich gemacht werden sollten. In Usenet-Gruppen ist es am einfachsten, die Mailadresse in der Form `benutzer@DIESEN_TEIL_LÖSCHEN_firma.com` zu hinterlassen. Menschen wissen, dass der eingefügte Text entfernt werden muss. Ein Spambot weiß das nicht, obwohl E-Mail-Harvester immer ausgeklügelter werden und diese Strategie immer besser überwinden können.

Auf Websites, die für die Öffentlichkeit gedacht sind, ersetzen Sie in E-Mail-Hyperlinks die einzelnen Buchstaben durch den entsprechenden ASCII-Code. Als Beispiel dient eine Adresse in einem mailto:-Eintrag einer Webseite im Klartext:

```
<a href="mailto:Sales@Company.com">Klicken Sie hier, um
➥Kontakt zur Vertriebsabteilung aufzunehmen.</a>
```

Einen einfachen ASCII-Codierer finden Sie unter www.wbwip.com/wbw/emailencoder.html. Wenn ASCII-Ziffern anstelle der Buchstaben verwendet werden, sieht die E-Mail-Adresse so aus:

```
<a href="mailto:&#115;&#097;&#108;&#101;&#115;&#064;&#099;&#111;
➥&#109;&#112;&#097;&#110;&#121;&#046;&#099;&#111;&#109">
```

Bestätigung ihrer Adresse

Bestätigte Adressen sind wertvoller als unbestätigte. Deshalb enthalten HTML-E-Mails wie im folgenden Beispiel häufig Hyperlinks zu Grafikdateien:

```
<img alt="Wild Times" arc="http://wildwildwild.biz/images/
➥wildtimes27.gif">
```

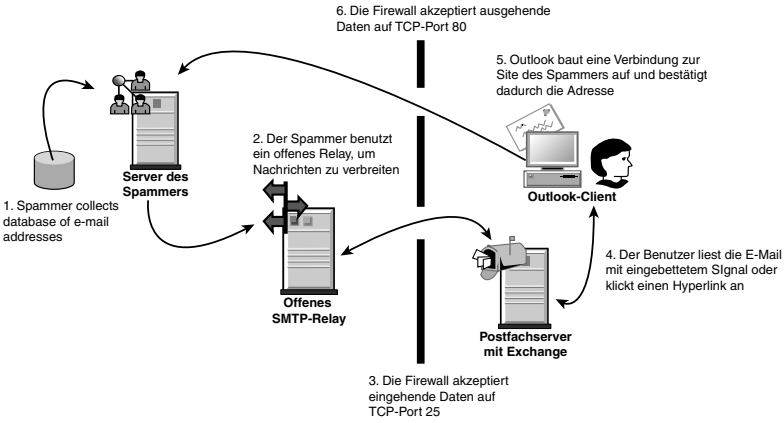
Wenn der Benutzer die Nachricht öffnet, dann lädt die E-Mail-Anwendung die Grafik von der Website des Spammers herunter und gibt auf diese Weise Informationen über den Benutzer an den Spammer weiter. Solche Hyperlinks werden Beacons (Signale) genannt, weil sie den Spammer benachrichtigen, dass der Benutzer tatsächlich existiert. In Outlook 2003, Outlook Express unter Windows XP mit SP 2 und Outlook Web Access 2003 werden eingebettete Grafiken nicht automatisch heruntergeladen. Das Ergebnis sehen Sie in folgender Abbildung.

Outlook 2003: Ein Beispiel für eine Nachricht bei der Signale blockiert werden. Anstelle des blockierten Links zu einer Grafik wird ein Platzhalter angezeigt

Die Blockierung von Signalen bringt auch Nachteile. Manche gängigen Systeme zur Nachrichtenverfolgung betten Grafiken in ausgehende Nachrichten ein. Wenn der Empfänger die Nachricht öffnet, baut der E-Mail-Client eine Verbindung zur verlinkten Grafik auf und schickt eine Bestätigung an den Absender. Blockiert der Client den Zugriff auf die Ziele von Hyperlinks, dann funktioniert dieses System nicht mehr. Der Empfänger hat in diesem Fall nur die Möglichkeit, den Korrespondenzpartner in eine Liste akzeptierter Absender (Whitelist) aufzunehmen.

4.4.2 Offene SMTP-Relays

Sobald ein Spammer ein paar hunderttausend E-Mail-Adressen gesammelt hat, sucht er eine Möglichkeit, ungehindert Nachrichten dorthin verschicken zu können. Ein SMTP-Server, der eingehende E-Mails akzeptiert und sie ohne Berücksichtigung des Ziels weiterleitet, wird zu einem offenen Relay. Wie ein solches Relay funktioniert, ist in folgender Abbildung zu sehen.



Spam: Versenden über ein offenes Relay.

Der SMTP-Dienst in Windows erlaubt anonymen Entitäten nicht, als Relay zu dienen. Nur Entitäten mit den Anmeldeinformationen einer Domäne können E-Mails weiterleiten, wodurch SMTP-Server außerhalb der Organisation im Wesentlichen blockiert werden.

Offene SMTP-Relays sind heutzutage recht selten geworden, doch offene Proxyserver sind für Spammer eine Alternative. Viele Würmer und Viren enthalten einen Proxydienst. Dadurch geben sie Spammern und Virenprogrammierern die Möglichkeit, auf ein System zuzugreifen und es als Sprungbrett zu nutzen. Spammer finden offene Relays und Proxys, indem sie Rechner suchen, die auf allgemeinen Ports reagieren, und diese Ports dann mit SMTP-Relayanfragen und HTTP CONNECT-Proxyanfragen testen. Diese Tests können Sie auch selbst auf der öffentlichen Schnittstelle Ihrer Server durchführen.

Hinweis: Lassen Sie sich immer erst eine schriftliche Erlaubnis Ihrer Vorgesetzten geben, ehe Sie Sicherheitstests durchführen.

SMTP-Relayanfrage

Bauen Sie mit der folgenden Syntax eine Verbindung vom öffentlichen Teil ihres Netzwerks zum öffentlichen Exchange-Server über Telnet auf:

```
telnet <Servername> 25
```

Der Server sollte mit einer SMTP-Nachricht reagieren, die ungefähr so aussieht:

```
220 EX1 Microsoft ESMTP MAIL Service, Version:6.0.3790.0
➥ready at Wed, 4 Feb 2004 14:32:31 -0700
```

Wenn Sie jetzt `EHLO` (Extended Hello) eingeben, erhalten Sie eine Liste der SMTP-Kapazitäten. Wenn der Server antwortet, verwenden Sie drei SMTP-Be-

fehle MAIL FROM, RCPT TO und DATA mit der folgenden Syntax, um eine Nachricht zu verschicken:

```
mail from: totallybogus@fabricatedaddress.biz
250 2.1.0 totallybogus@fabricatedaddress.biz....Sender OK
rcpt to: someusername@yahoo.com
250 2.1.5 someusername@yahoo.com
data
354 Start mail input; end with <CRLF>.<CRLF>
Subject: Your assistance most graciously and desperately needed
Let me introduce myself. I am the grandson of the Duke of
Earl and I need your help.
.
250 2.6.0 EX-S1HM3SOlbpH71y00000008@ex1.actualsmptdomain.com
Queued mail for delivery
quit
221 2.0.0 ex1.actualsmtpdomain.com Service closing
➥transmissionchannel
Connection to host lost.
```

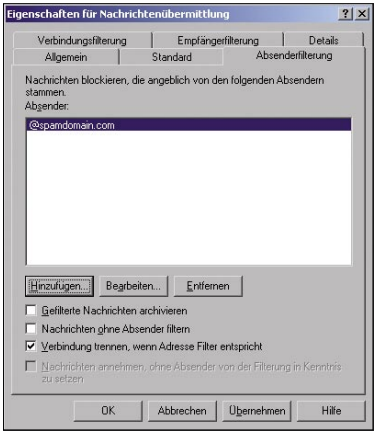
Akzeptiert ein Server eine RCPT TO-Adresse außerhalb seiner SMTP-Domäne, dann haben Sie ein offenes Relay gefunden.

Der Test auf offene Proxys ist etwas komplizierter und nur mit speziellen Programmen durchzuführen, z.B. mit Proxy Analyzer von G-Lock Software (www.glocksoft.com). Richten Sie Proxy Analyzer auf einen Computer aus und geben Sie an, welche Ports eventuell anfällig sein könnten. Warten Sie dann ab, ob das Programm zu diesen Ports als Proxy Verbindung aufnehmen kann. Enthalten ist auch ein Bewertungssystem, mit dem Sie bestimmen können, wie anfällig ein Rechner für Angriffe ist.

4.4.3 Blockieren bekannter Spammer

Verwenden Sie die Informationen von Spamhaus (www.spamhaus.org) und dem Spamhaus-Register bekannter Spam-Unternehmen (Spamhaus Register of Known Spam Operations, ROKSO) unter www.spamhaus.org/rokso/index.lasso, um Spamversender zu identifizieren. Unter www.spamsites.org/live_sites.html finden Sie auch eine textbasierte Liste mit SMTP-Domänen und Ländern, in denen Spammer agieren. Diese Listen können Sie dann mit Hilfe der Optionen für die Nachrichtenzustellung wie folgt in Exchange importieren.

In Exchange gibt es verschiedene Möglichkeiten, eingehende Nachrichten nach der SMTP-Domäne oder der IP-Adresse des Senders bzw. durch Nachschlagen bei einem Provider für Spamidentifizierungsdienste zu filtern. Die Filter können Sie in ESM über GLOBALE EINSTELLUNGEN/NACHRICHTENÜBERMITTLUNG einrichten. Das Fenster EIGENSCHAFTEN sehen Sie in folgender Abbildung.



Absenderfilterung: Das Fenster listet die blockierten SMTP-Domänen auf.

Wenn Sie alle Mails von einer bestimmten Domäne blockieren möchten, verwenden Sie die Syntax `*@spamdomain.com`. `Spamdomain` steht hier für die SMTP-Domäne, die Sie blockieren möchten. Sie können dem Filter beliebig viele Domänen hinzufügen. Die Option NACHRICHTEN OHNE ABSENDER LÖSCHEN beseitigt E-Mails ohne Absenderadresse.

Ist die Option VERBINDUNG TRENNEN, WENN ADRESSE FILTER ENTSPRICHT aktiviert, dann schickt der Server an diese Adresse keine Nachricht, wenn die E-Mail nicht zugestellt werden konnte. So wird verhindert, dass die Adresse bestätigt wird und noch mehr Spam erhält.

Einrichten eines virtuellen SMTP-Server

Vorhandene Filter sind nicht automatisch wirksam. Vielmehr müssen Sie jeden virtuellen SMTP-Server wie folgt einrichten, damit er die Filter verwendet:

1. Starten Sie ESM und suchen Sie im Container eines Servers nach PROTOKOLLE/ SMTP.

2. Öffnen Sie das Fenster EIGENSCHAFTEN für den virtuellen SMTP-Standardserver.

3. Klicken Sie auf der Registerkarte ALLGEMEIN auf ERWEITERT. Dann öffnet sich das gleichnamige Fenster aus unten folgender Abbildung mit einer Liste der IP-Adressen und Ports, die dem virtuellen Server zugeordnet sind.

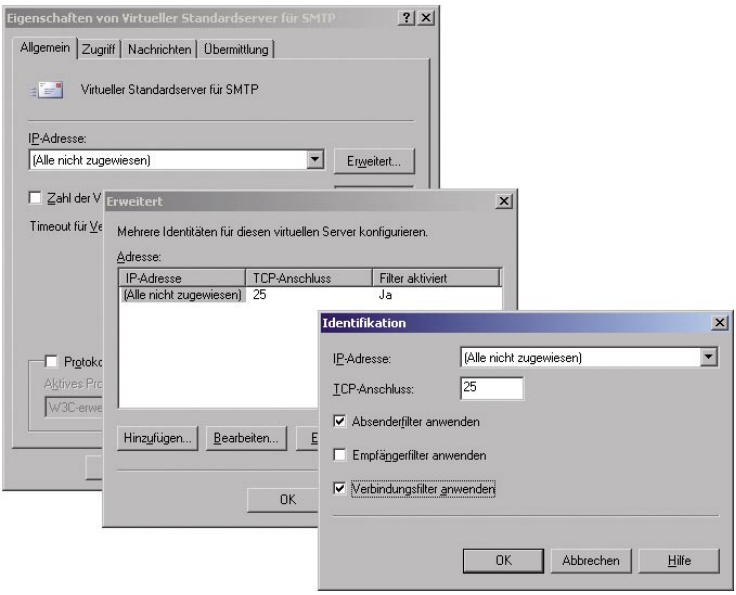
4. Klicken Sie auf BEARBEITEN. Das Fenster IDENTIFIKATION öffnet sich.

5. Aktivieren Sie das Kontrollkästchen ABSENDERFILTER ANWENDEN>> und klicken Sie auf OK.

6. Bestätigen Sie mit OK. Das Fenster ERWEITERT wird geschlossen. Klicken Sie ein weiteres Mal auf OK, um die Einstellungen zu speichern.

7. Führen Sie diesen Vorgang für alle virtuellen SMTP-Server durch, auf denen der Filter angewendet werden soll.

Prüfen Sie anschließend nach, ob der Filter einwandfrei funktioniert. Dazu versuchen Sie, über Telnet eine Verbindung zu dem Server so aufzunehmen, als ob sie von einer blockierten SMTP-Domäne käme.



Sperre: So richten Sie einen Verbindungsfilters auf einen virtuellen SMTP-Server ein.

4.4.4 Echtzeit-Blockierlisten

Wenn Sie in einen solchen Filter sehr viele SMTP-Domänen aufnehmen, haben Sie ein Problem: Sie müssen sich dauernd um diese Liste kümmern. Da ist es wesentlich einfacher, auf die Dienste von Organisationen zurückzugreifen, die den Missbrauch von SMTP-Servern permanent überwachen, also auf so genannte RBLs. Für die Abkürzung gibt es unterschiedliche Erklärungen. Microsoft verwendet die Bezeichnung Real-Time Block List, andere Möglichkeiten sind Real-Time Blackhole List oder Real-Time Boycott List.

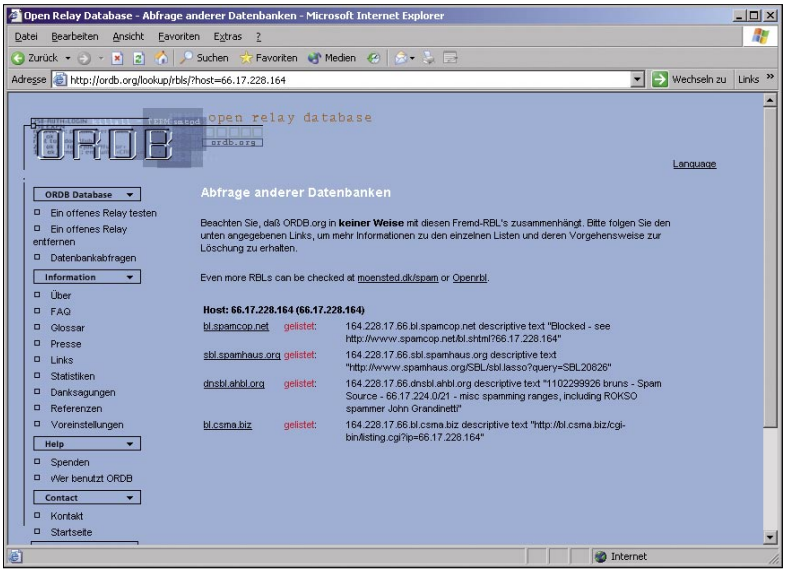
Auch wenn die Bezeichnungen unterschiedlich sind, haben alle RBL-Anbieter dasselbe Ziel, was den Missbrauch von SMTP betrifft: Finden, Herkunft identifizieren und die Öffentlichkeit informieren. Sie blockieren Spam nicht im üblichen Sinn, d.h. durch Bereitstellung eines Filters. Damit wären sie juristisch angreifbar. Stattdessen erstellen sie Listen und geben diese an Sie weiter, damit Sie das Filtern übernehmen können. Weder Sie selbst noch der RBL-Anbieter unternimmt offen etwas gegen die Server der Spammer.

Am bekanntesten ist MAPS (Mail Abuse Prevention System), ein gebührenpflichtiger Provider, zu dem es unter der Adresse www.mail-abuse.org weiterführende Informationen gibt. Zu den kostenlosen Providern gehören:

- DSBL (Distributed Server Boycott List, www.dsbl.org)
- ORDB (Open Relay Database, www.ordb.org)
- SpamCop (www.spamcop.net)
- NJABL (Not Just Another Bogus List, www.njabl.org)

RBL-Anbieter

Eine komplette Liste von RBL-Anbietern finden Sie auf der Website von Declude unter www.declude.com/junkmail/support/ip4r.htm. Hier werden auch die Vor- und Nachteile der einzelnen RBLs beschrieben. Manche RBL-Anbieter bieten auf ihrer Website eine Möglichkeit, nach der SMTP-Domäne oder der IP-Adresse eines potenziellen Spammers zu suchen. Die Suchseite von ORDB, zu finden unter www.ordb.org/lookup, gibt Ihre Anfrage an zahlreiche Sites weiter und liefert einen ausführlichen Bericht zurück.



Detailliert: ORDB zeigt das Ergebnis einer umfassenden Suche nach der IP-Adresse eines möglichen Spammers an.

Einige Anbieter geben an ihre Kunden eine Textdatei mit Hinweise zu bekannten Spamsites weiter, die auf den lokalen Mailservern des Kunden in einen Filter geladen werden kann. Solche Blockierlisten können lang sein und müssen regelmä-

ßig aktualisiert werden, aber im Vergleich zu anderen Methoden ist eine lokale Filterung am schnellsten. Der RBL-Anbieter liefert eine Anleitung, wie die Liste in die gängigen E-Mail-Server geladen werden kann, einschließlich Exchange.

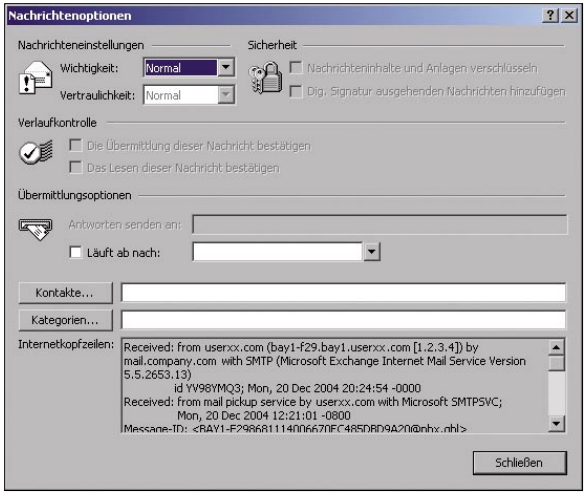
Bei den meisten Anbietern müssen Sie eine Erklärung unterzeichnen, dass Sie die Liste ausschließlich für eigene Zwecke nutzen und den Inhalt nicht veröffentlichen. Dadurch sind Sie und der Anbieter vor rechtlichen Schritten geschützt.

4.4.5 Reverse-DNS-RBL-Dienste

Bei den meisten RBL-Anbietern gibt es einen Online-Suchservice, auf den Sie ohne besondere Clients über eine Reverse-DNS-Anfrage zugreifen können. Um den RDNS-Dienst zu nutzen, senden Sie eine DNS-Anfrage, die die umgekehrte IP-Adresse des verdächtigen Servers enthält, gefolgt vom RDNS-Domänennamen des Anbieters, für ORDB also etwa `relays.ordb.org`. Der RDNS-Dienst gibt einen A-Eintrag mit einer IP-Adresse in der Form 127.0.x zurück. Der Platzhalter steht hier für ein bestimmtes unerwünschtes Verhalten. Die Codes der Provider sind nicht einheitlich. Bei NJABL etwa haben sie folgende Bedeutung:

- 127.0.0.2 – Offene Relays
- 127.0.0.3 – DFÜ/dynamische IP-Bereiche
- 127.0.0.4 – Spamquellen
- 127.0.0.5 – Offene Relays mit mehreren Stufen
- 127.0.0.8 – Systeme mit offenen CGI-Skripts, die sie zu offenen Relays werden
- 127.0.0.9 – Offene Proxyserver

SMTP-Infos: Aus den Optionen für eine Nachricht in Outlook



Angenommen, Sie erhalten eine Nachricht, die Sie für Spam halten. Sie können die IP-Adresse des Absenders bestimmen, indem Sie sich die Header ansehen. Klicken Sie in Outlook mit der rechten Maustaste auf die Nachricht und wählen Sie OPTIONEN aus dem Kontextmenü. Dann öffnet sich das Fenster NACHRICHTENOPTIONEN, welches in unten stehender Abbildung dargestellt ist. Informationen über den SMTP-Server, der die Nachricht abgeschickt hat, finden Sie im Feld INTERNETKOPFZEILEN. Die einzigen wirklich vertrauenswürdigen Informationen über die Header stehen im Feld RECEIVED FROM. Alles andere kann vom Absender gefälscht sein – und ist es vermutlich auch.

Reverse-DNS Beispiel

In diesem Beispiel hat der SMTP-Server des Absenders die IP-Adresse 1.2.3.4. Wenn Sie diese Adresse mit RDNS überprüfen möchten, starten Sie mit Nslookup eine DNS-Anfrage. Ich verwende in diesem Beispiel den Anbieter NJABL. Die RDNS-Lookupanforderung hat die folgende Syntax:

```
C:\>nslookup 4.3.2.1.dnsbl.njabl.org
Nicht-autorisierende Antwort:
Name: 4.3.2.1.dnsbl.njabl.org
Address: 127.0.0.9
```

Der Rückgabecode 127.0.0.9 zeigt an, dass die E-Mail von einem offenen Proxyserver abgeschickt wurde, dessen Besitzer möglicherweise keine Ahnung davon hat, dass sein Server zum Versand von Spam verwendet wird.

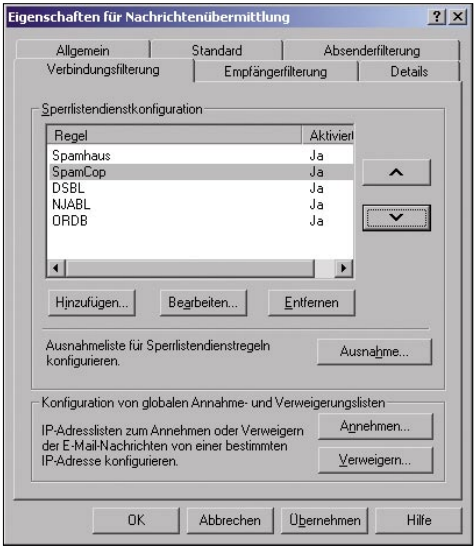
Wenn Sie sich die Rückgabecodes nicht merken möchten, verwenden Sie Nslookup im interaktiven Modus, um einen TXT-Eintrag zu erhalten, der dem A-Eintrag entspricht. Die Syntax sieht wie folgt aus:

```
C:\>nslookup
> set type=txt
> 4.3.2.1.dnsbl.njabl.org
Nicht-autorisierende Antwort:
4.3.2.1.dnsbl.njabl.org text =
?open proxy - 1058170803?
```

4.4.6 Einrichten eines Verbindungsfilters für einen RDNS-RBL-Anbieter

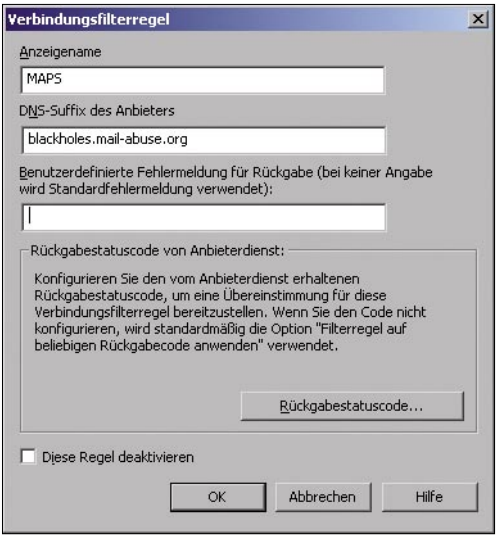
Sie brauchen nur ein paar Minuten, um Exchange 2003 für die Verwendung eines RDNS-Dienstes zu konfigurieren. Starten Sie ESM und gehen Sie zu GLOBALE EINSTELLUNGEN, öffnen Sie das Eigenschaftenfenster für das Objekt NACHRICHTENÜBERMITTLUNG und wählen Sie dort die Registerkarte VERBINDUNGSFILTERUNG aus.

Verbindungsfilter: Wählen Sie einen Reverse-DNS-RBL-Anbieter auf der Liste aus.

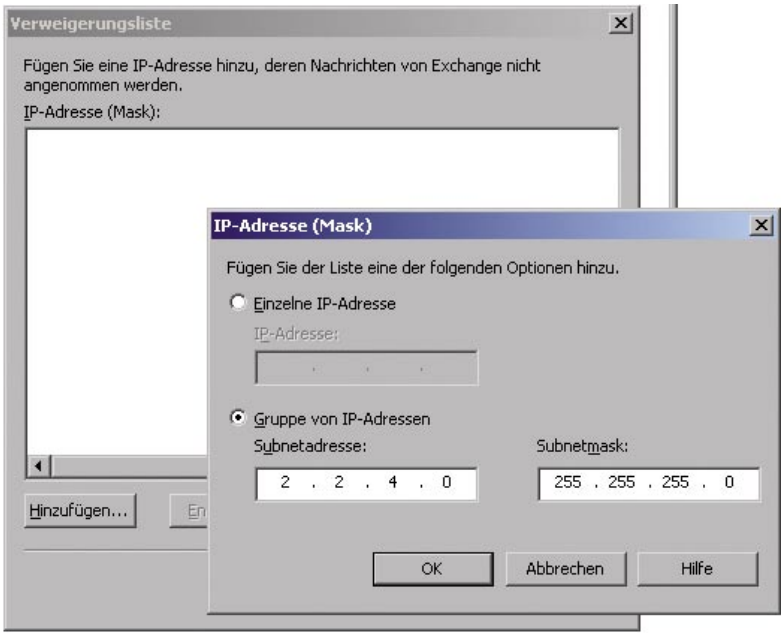


Um eine neue Filterregel zu erstellen, klicken Sie auf HINZUFÜGEN. Füllen Sie das Feld ANZEIGENAME aus und geben Sie dann das RDNS-Suffix des Anbieters an. Diese Informationen finden Sie auf dessen Website. Die Einstellungen für die Fehlermeldung lassen Sie unverändert.

Neuer Anbieter: So erstellen Sie einen Verbindungsfilterregel mit einem neuen Reverse-DNS-RBL-Anbieter.



Wenn Sie eine unerwünschte Mail von einem SMTP-Server erhalten, der noch nicht als Spamversender identifiziert wurde, können Sie seine IP-Adresse mit der Option KONFIGURATION VON GLOBALEN ANNAHME-UND VERWEIGERUNGSLISTEN in den Verbindungsfilter eintragen. Klicken Sie auf VERWEIGERN, um das Fenster VERWEIGERUNGSLISTE zu öffnen, und dann auf HINZUFÜGEN, um eine einzelne IP-Adresse oder einen Adressbereich anzugeben. Ein Beispiel ist in folgender Abbildung zu sehen.



Blockade: Fügen Sie die IP-Adressen eines neuen Spammers zu einer Liste gesperrter Adressbereiche zu.

Übernehmen des Verbindungsfilters für die virtuellen SMTP-Server

Wenn Sie in einem Verbindungsfilter einige RDNS-Anbieter definiert haben, übernehmen Sie ihn für die virtuellen SMTP-Server wie folgt:

1. Starten Sie ESM und suchen Sie im Server-Container nach PROTOKOLLE/ SMTP.

2. Öffnen Sie das Eigenschaftenfenster für den virtuellen SMTP-Standardserver.

3. Rufen Sie die Registerkarte ALLGEMEIN auf und klicken Sie auf ERWEITERT. Das Fenster ERWEITERT öffnet sich und zeigt die verschiedenen IP-Adressen und Ports an, die dem Server zugeordnet sind.

4. Klicken Sie auf BEARBEITEN. Das Fenster IDENTIFIKATION wird geöffnet.

5. Aktivieren Sie VERBINDUNGSFILTER ANWENDEN, bestätigen Sie mit OK und klicken Sie dann nochmals auf OK, um die Einstellungen zu speichern.

6. Führen Sie diesen Vorgang für jeden virtuellen SMTP-Server durch, für den der Filter gelten soll.

Grenzen der RBLs

RBL-Filter an sich bieten keinen umfassenden Schutz vor Spam. Zuallererst deshalb, weil nicht alle Spam von offenen Relays bzw. Proxys verschickt wird. Zweitens kennen Spammer alle möglichen Tricks, um von einem Rechner auf den nächsten zu wechseln. Dadurch verschickt keiner der genutzten Rechner so viel Spam, dass die RBL-Anbieter auf ihn aufmerksam werden.

Aber das Hauptproblem bei der Verwendung von RBL-Filtern sind die vielen falschen Einträge. Von einer gesperrten SMTP-Domäne, die ein Spammer missbraucht, kommen oft auch erwünschte Mails, und manchmal landet eine IP-Adresse ohne Grund bzw. aus Versehen auf der Liste.

Wenn Ihre Organisation in eine RBL aufgenommen wird, geben die Abonnenten Ihre Mails an den RBL-Dienst weiter. Je nach den Filtereinstellungen des Absenders werden Sie von der Sperrung möglicherweise gar nicht informiert. Dadurch wird verhindert, dass es während eines Wurmangriffs im Internet zu Ausfällen in größerem Umfang kommt. Aber es führt auch dazu, dass sich die Benutzer in Ihrer Organisation fragen, warum niemand mehr auf ihre E-Mails antwortet.

Sobald Sie die Ursache für die Aufnahme in die RBL behoben haben, nehmen Sie Kontakt mit dem Anbieter auf, damit der Eintrag wieder entfernt wird. RBL-Anbieter stehen jedoch nicht regelmäßig in Kontakt miteinander, weshalb es vermutlich nicht ausreicht, nur einen anzusprechen. Wenn Ihr Name aus der Datenbank einer RBL gelöscht werden soll, dann kann das eine Woche und länger dauern. Versuchen Sie nicht, den RBL-Anbieter zu schnellerem Arbeiten zu zwingen. Die Mitarbeiter dort haben den ganzen Tag von morgens bis abends mit rücksichtslosen Spammern zu tun und brauchen eine Jabba-the-Hutt-Mentalität. Sie fürchten weder Drohungen von Ihnen noch von Ihrem Geschäftsführer oder Ihrem Rechtsanwalt. Wenn Sie den gängigen SMTP-Anforderungen genügen, haben Sie gute Chancen, aus der Liste gelöscht zu werden.

4.4.7 Blockierung durch Challenge-Response

Eine Möglichkeit, Spam zu hundert Prozent zu sperren, besteht darin, alle unbekannten Absender zur Identifizierung zu zwingen. Bei diesem Ansatz wird ein Dienstanbieter verwendet, der alle eingehenden Nachrichten filtert. Erhält er eine E-Mail von einem Absender, der vorher noch nie eine Nachricht geschickt hat, dann isoliert er sie und sendet eine Herausforderung an den Absender zurück, auf die letzterer reagieren soll.

Welche Reaktion gefordert wird, hängt vom Hersteller ab. SpamLion (www.spamlion.com) bittet den Absender etwa, einen Hyperlink anzuklicken. Das ähnelt den Registrierungsüberprüfungen von Mailinglistenmanagern wie Majordomo. Bei SpamArrest (www.spamarrest.com) muss der Absender eine Bitmap-Datei lesen, die ein Wort darstellt, und dieses Wort in die Antwortmail eingeben.

Solche Systeme sind ungewöhnlich leistungsfähige Filter, bieten aber nicht immer die optimale Lösung. Dies ist vor allem dann der Fall, wenn erwünschte Nachrichten nicht von Menschen verschickt werden. Ein Paradebeispiel sind abonnierte Mailinglisten, ebenso wie Firmen-E-Mails, die wichtige Produktinformationen für Kunden enthalten. Die wenigsten Betreiber einer Mailingliste machen sich die Mühe, auf Herausforderungsnachrichten zu reagieren. Die Folge davon ist, dass möglicherweise wichtige Informationen nie beim Empfänger ankommen. Wenn dieser sich nicht die Zeit nimmt und den Domänennamen einer Mailingliste im Voraus freischaltet, dann wandern die E-Mails dieser Liste direkt in den Papierkorb.

Ein weiteres Problem bei diesem Ansatz besteht darin, dass die Kunden, die ein System nutzen, von der Qualität seiner Messaginginfrastruktur abhängig sind. Wenn das System zusammenbricht, wegen Überlastung nicht vorübergehend oder dauerhaft erreicht werden kann oder durch einen globalen verteilten DoS-Angriff (Denial of Service) zum Stillstand gebracht wird, dann kommt beim Kunden der gesamte E-Mail-Verkehr zum Erliegen.

4.4.8 Signaturbasierte Filter

Eine weitere Möglichkeit, Spam und Viren auszufiltern, besteht darin, den Inhalt einer Nachricht zu untersuchen und dann mit einer Kombination aus Schlüsselwörtern, Regeln und Inhaltsanalyse zu bestimmen, ob die Nachricht „spammig" ist oder möglicherweise einen Virus enthält.

Wenn der Hersteller die Regeln häufig aktualisiert, kann dieser Ansatz äußerst effektiv sein. Eine auf Regeln basierende Filterung wird jedoch dadurch eingeschränkt, dass schädliche Inhalte sehr verschieden aussehen können. Ein regelbasierter Antispamfilter entdeckt vielleicht eine Nachricht mit der Betreffzeile „You Can Last Twice as Long", aber übersieht „You, Can La$t Twice /As Long mxplxct". Ein anderes Beispiel: Eine Virusmail wird dann entdeckt, wenn sie eine VBS-Datei enthält, bleibt aber unter Umständen unerkannt, wenn stattdessen eine ZIP-Datei angehängt ist.

Fast alle Antivirenprogramme nutzen Signaturen in irgendeiner Form. Die Beispiele dafür sind zu zahlreich, als dass man sie hier anführen könnte. Qualitätsunterschiede zeigen sich bei signaturbasierten Lösungen oft darin, wie schnell Signaturen zur Verfügung stehen bzw. ein neuer Angriff erfasst und in die Signaturdatei aufgenommen werden kann und wie einfach sich die Signaturen innerhalb eines Unternehmens weitergeben lassen.

Auch einige Hersteller von Antispamprogrammen nutzen Signaturen, weil ihr Ergebnis vorhersagbar und der Verteilungsmechanismus bekannt ist. Auf Regeln beruhen unter anderem die folgenden verbreiteten Antispamprodukte:

- iHateSpam von Sunbelt Software (www.sunbeltsoftware.com)
- MailMarshal von NetIQ (www.netiq.com)
- SurfControl von SurfControl (www.surfcontrol.com)

4.4.9 Hashbasierte Filter

Antiviren- und Antispamprogramme, die auf Signaturen basieren, blockieren möglicherweise auch erwünschte E-Mails, die dem Filtermechanismus verdächtig vorkommen. Hashbasierte Filter versuchen diesen Fehler zu vermeiden, indem sie einzelne Exemplare unerwünschter Nachrichten abfangen und auf einen digitalen Fingerabdruck, Hash genannt, reduzieren. In der Kryptographie wird ein Hash aus einer unidirektionalen Funktion mit einer Ausgabe fester Länge konstruiert, die sehr empfindlich auf die Eingabe reagiert. Bei einer guten Hashfunktion wird durch ein einziges verändertes Byte in der Eingabe der Hashinhalt zu 50 Prozent modifiziert. Ein Anbieter eines hashbasierten Programms ist bemüht, Spam und Viren zu bekommen. Wenn der unerwünschte Inhalt bestätigt ist, wird ein Hash produziert und eine Aktualisierung verschickt. Die Clients erhalten den Hash und prüfen damit eingehende Nachrichten.

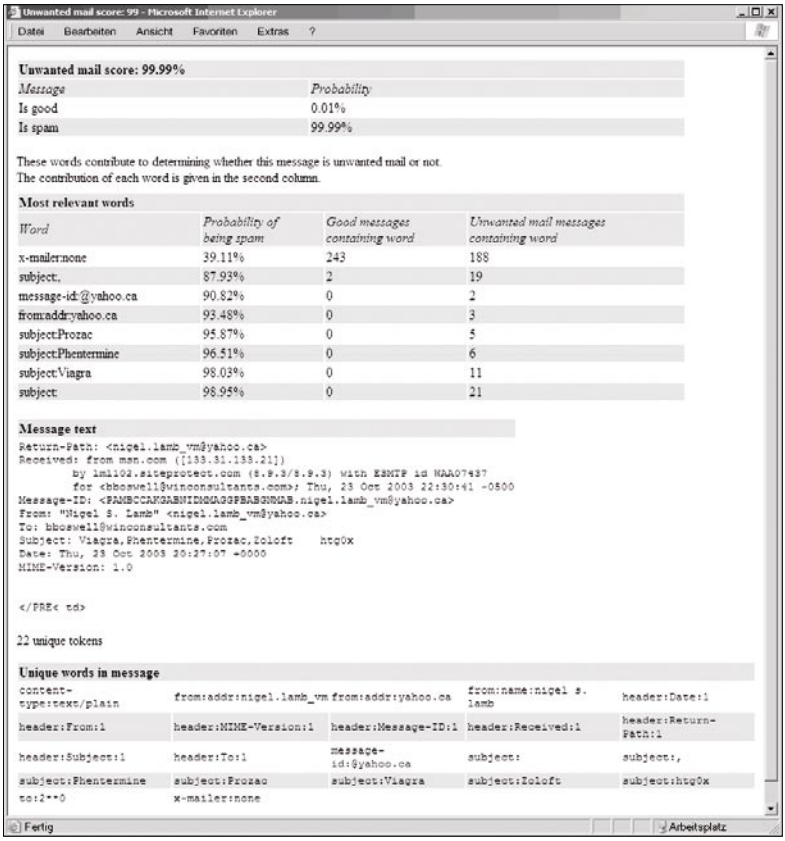
Im Vergleich zur Verwendung von Signaturen haben hashbasierte Filter etliche Vorteile. Sie sind sehr schnell, weil Hash-Algorithmen auf Leistung optimiert sind, und praktisch unfehlbar, denn es ist schlicht unmöglich, dass zwei Nachrichten in freier Wildbahn den gleichen Hash haben. Da ein Hash auch sehr kompakt ist, lassen sich Aktualisierungen schnell und einfach an die Clients verschicken.

Aber ein hashbasierter Filter hat auch einen großten Nachteil. Wenn der Anbieter nicht bemerkt, dass eine Virenattacke einsetzt oder eine neue Spam-E-Mail abgeschickt wird, sind die Clients den unerwünschten Nachrichten ausgeliefert. Ein Beispiel für ein hashbasiertes Tool ist die Software Brightmail Anti-Spam von Brightmail (www.brightmail.com).

4.4.10 Bayes-Filter

Im Kampf gegen schwer zu fassende Spam-E-Mails nutzen viele Anbieter von Antispamprogrammen einen Entscheidungsprozess, der auf den Arbeiten von Thomas Bayes beruht, einem Mathematiker und Theologen des 18. Jahrhunderts. In einem Text mit dem Titel „Essay Towards Solving a Problem in the Doctrine of Chances“ stellte Reverend Bayes die These auf, dass es möglich sei, anhand der Häufigkeit eines Ereignisses in der Vergangenheit die Wahrscheinlichkeit seines Auftretens in der Zukunft zu berechnen.

Bayes' Logik definiert den Prozess, in dem ein naiver Lernender Kenntnisse über einen Sachverhalt gewinnt. Ein Spamfilter, der diese Entscheidungsprozesse verwendet, muss also den Unterschied zwischen erwünschter E-Mail und Spam lernen. Das dauert ein wenig. Die meisten Bayes-Filter zerlegen den Inhalt einer Nachricht in Token und analysieren, wie oft ein bestimmter Token in bekannten Spam-E-Mails verwendet wurde. Das Ergebnis einer Bayes-Analyse für eine Spam-E-Mail, durchgeführt von InBoxer, einem Outlook-Plug-In von Audiotrieve (www.audiotrieve.com), ist in folgender Abbildung dargestellt. Wie Sie sehen können, hat der Filter bemerkt, dass es sich bei der Nachricht mit einer Wahrscheinlichkeit von 98,03 Prozent um Spam handelt, weil das Wort „Viagra" bereits in elf unerwünschten Mails enthalten war. In Verbindung mit einer leeren Betreffzeile (auch fast immer ein Zeichen von Spam) trifft er die Entscheidung, die Nachricht zu sperren.



Inboxer: Bewertung einer E-Mail von Inboxer, einer Anwendung mit Bayes-Filtern

Durch die tokenbasierte Analyse sind Bayes-Filter besonders gut im Identifizieren von Mails, die gewollte Falschschreibungen enthalten. Ein regelbasierter Filter lässt sich möglicherweise von einem Satz wie „Kure baldne$$ with hare implant$“ täuschen, aber ein Bayes-Filter weiß, dass Token mit Sonderzeichen fast immer auf Spam hinweisen, und ordnet die E-Mail entsprechend ein. Wenn die Nachricht jedoch sorgfältig verfasst ist, wird auch ein Bayes-Filter nicht aktiv. Außerdem verzichten viele Spammer ganz auf Worte und verschicken stattdessen E-Mails mit eingebetteten Grafiken, bei denen eine Bayes-Analyse nicht möglich ist. Solche Nachrichten werden aber von Outlook Web Access und Outlook 2003 blockiert. Weitere Antispam-Programme mit Bayes-Filtern sind:

- MailEssentials für Exchange/SMTP von GFI Software (www.gfi.com)
- OutlookSpamFilter von Novosoft (www.novosoft.com), ein Outlook-Plug-In
- SpamKiller von McAfee (www.mcafee.com, beruht auf der legendären Technologie von Spam-Assassin)

4.4.11 Randfilter

Sie können einen Antispamfilter auf einem Front-End-Server mit SMTP installieren. Er überwacht den ein- und ausgehenden SMTP-Verkehr Ihrer Organisation und weist verdächtige Mails entweder ab oder markiert sie. Dadurch wird verhindert, dass sich auf Ihren Servern Spam ansammelt und Speicherplatz verbraucht. Ein Randfilter überwacht den gesamten Verkehr, und wenn er Bayes-Filter verwendet, lernt er rasch die typischen Muster von Spam-E-Mails.

Sie können einen Smarthost (einen Front-End-SMTP-Server) mit einem Antispamprogramm einrichten, der Nachrichten sperrt oder mit einer Spambewertung versieht. Diese Bewertung nutzen Exchange-Server oder Outlook-Clients, um Nachrichten nach dem entsprechenden Attribut auszufiltern. Exchange 2003 enthält einige benutzerdefinierte Ereignisnachrichtensenken, die Antispamprogramme zum Filtern einsetzen können. Der neue Intelligent Message Filter (IMF) von Microsoft verwendet diese Ereignisnachrichtensenken zusammen mit regelbasierter Überprüfung und einer Matrix zur Entscheidungsfindung, um Spam zu markieren und zu beseitigen. Zu den unter Windows laufenden SMTP-Randfiltern gehören folgende:

- OrangeBox Mail von Cobion (www.cobion.com)
- MailSweeper SMTP Edition von Clearswift (www.clearswift.com)
- Trend InterScan Message Security Suite (www.trendmicro.com)

Auch ein externer Dienstleister ist ein Randfilter, der alle ein- und ausgehenden Mails durch sein System leitet und nach Spam und Viren untersucht. Da ein solcher Dienstleister Millionen von E-Mails prüft, lernen die Filter die Spamsignaturen sehr schnell und arbeiten dadurch effizient und effektiv. Beispiele für externe Dienstleister sind:

- MessageLabs (www.messagelabs.com)
- Postini (www.postini.com)

Wenn in Ihrer Organisation Sicherheit, Datenschutz oder Zuverlässigkeit eine große Rolle spielen, dann sollten Sie vor Abschluss eines Vertrages eingehend Rücksprache mit dem Vertreter des Dienstleisters halten, um sicherzustellen, dass Sie den Dienst problemlos abbestellen können, wenn er Ihren Anforderungen nicht entspricht.

4.4.12 Speicherfilter

Wenn es in Ihrem Budget keinen Spielraum für weitere Server, mehrstufige Firewalls oder externe Dienstleister gibt und Ihr öffentlich zugänglicher Exchange-Server hinter einer preisgünstigen Firewall steckt, die die Portweiterleitung für eingehenden SMTP-Verkehr durchführt, können Sie auf Speicherfiltern beruhende Antispam- oder Antivirenprogramme verwenden. Die meisten bekannten Anbieter von Antivirenprogrammen bieten auch Programme zur Spamabwehr; wenn Sie beides kombinieren, nutzen Sie den Vorteil garantierter Kompatibilität und einen möglichen Preisnachlass. Produkte von einem Hersteller einzusetzen, bietet die beste Garantie für Stabilität und Leistungsfähigkeit.

Wenn Sie speicherbasierte Antiviren- und Antispamprogramme verschiedener Hersteller miteinander kombinieren, sollten Sie die Kompatibilität prüfen. Achten Sie dabei besonders auf die Quarantäneverfahren der beiden Anwendungen. Sie möchten sicher nicht, dass der Server instabil wird, weil sich beide Programme um eine Nachricht zanken, die wie Spam aussieht, aber einen Virus enthält.

4.4.13 Clientfilter

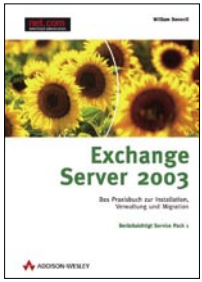
Auch wenn Sie sich dafür entscheiden, Rand- und Speicherfilter gegen Spam und Viren einzusetzen, sollten Sie immer zusätzlich noch Clientfilter verwenden. Oft ergänzen die Benutzer ihre dienstlichen Mails mit POP3-E-Mails von externen Mailservern. Mit clientbasierten Filtern erweisen Sie diesen Benutzern in jedem Fall einen guten Dienst.

Wenn Sie Clientfilter testen, achten Sie darauf, wo gesperrte Mails gespeichert werden. Verschiebt der Filter die Nachrichten einfach vom Posteingang des Benutzers in einen anderen Ordner auf dem Server, dann haben Sie zwar den Benutzern einen Dienst erwiesen, nicht aber sich selbst. Falls möglich, wählen Sie einen Clientfilter, der Spam entweder nach einer kurzen Zeit vollständig löscht oder in ein Repository auf dem lokalen Rechner verschiebt.

Kleine Firmen ohne Exchange-Server können auch die Junk-E-Mail-Filterung von Outlook verwenden. Outlook 2000 und die aktuelleren Versionen enthalten vorgefertigte Regeln zum Erkennen von Spam (Junk-E-Mails) und Pornographie.

In Outlook 2003 ist die Konfiguration mit der Schaltfläche JUNK-E-MAIL auf der Registerkarte EINSTELLUNGEN im Menü OPTIONEN relativ einfach. Den Filter können Sie mit Listen aus dem Internet einrichten. Eine solche Liste, die sich herunterladen und direkt in ein Outlook-Profil aufnehmen lässt, finden Sie zum Beispiel bei GazNET (www.gaznet.com). Outlook 2003 enthält auch einen intelligenten Filter, der über Office Update aktualisiert wird. (ala)

Weiterführende Infos



Unser Artikel zu Microsoft Exchange basiert auf dem Kapitel 13 des Standardwerks „Exchange Server 2003" von William Boswell aus dem Verlag Addison-Wesley. Sie können dieses über 850 Seiten starke Buch auch in unserem Buchshop (www.tecchannel.de) unter dem Webcode „buchshop" bestellen oder bequem als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Spam- und Virenabwehr mit Exchange	442764	S.144
Grundlagen: Filtermethoden für Spam	430603	–
Spam-Abwehr mit Linux	429776	–
Das Netz der Phisher: Wie Online-Betrüger arbeiten	447964	–
Sicherheitsrisiko Phishing	402413	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

4.2 Zentrales Windows-Management durch Gruppenrichtlinien

Viele Probleme, mit denen der Service Desk und Administratoren von Windows-Umgebungen zu tun haben, lassen sich bereits im Vorfeld vermeiden, wenn man die Gruppenrichtlinien nutzt. Denn oft ist die Ursache von Problemen eine versehentlich oder wissentlich geänderte Systemkonfiguration. Mit den Gruppenrichtlinien lassen sich Konfigurationseinstellungen aber zentral vorgeben. Windows sorgt dabei dafür, dass die Einstellungen spätestens beim nächsten Systemstart wieder auf den vorgegebenen Wert gesetzt werden. Und wenn das nicht reicht, kann man beispielsweise auch viele Bereiche der Systemsteuerung vor der Nutzung durch Anwender schützen.

Zu den Gruppenrichtlinien gibt es im Windows-Umfeld kaum Alternativen. Lösungen für das Client Lifecycle Management, also die Softwareverteilung, das Patch-Management und andere Aufgaben im Betrieb, unterstützen zwar oft die Anpassung von Registry-Einstellungen. Verglichen mit den Gruppenrichtlinien ist das aber mühselig und deckt nur einen Teil der Anforderungen ab. Genauso stoßen auch die Anwendungen für das Sicherheits-Management schnell an ihre Grenzen, da sich das Konfigurations-Management nicht auf einzelne Sicherheitseinstellungen reduzieren lässt.

Die Gruppenrichtlinien sind dagegen genau für diesen Einsatzbereich entwickelt worden – die zentrale Konfiguration von System- und Sicherheitseinstellungen in Windows-Netzwerken. Damit stellt sich nur noch die Frage, warum die Gruppenrichtlinien nicht in jedem Windows-Netzwerk intensiv genutzt werden. Die Antwort darauf ist einfach: Die Nutzung von Gruppenrichtlinien ist nicht leicht und setzt einiges an Vorüberlegungen voraus.

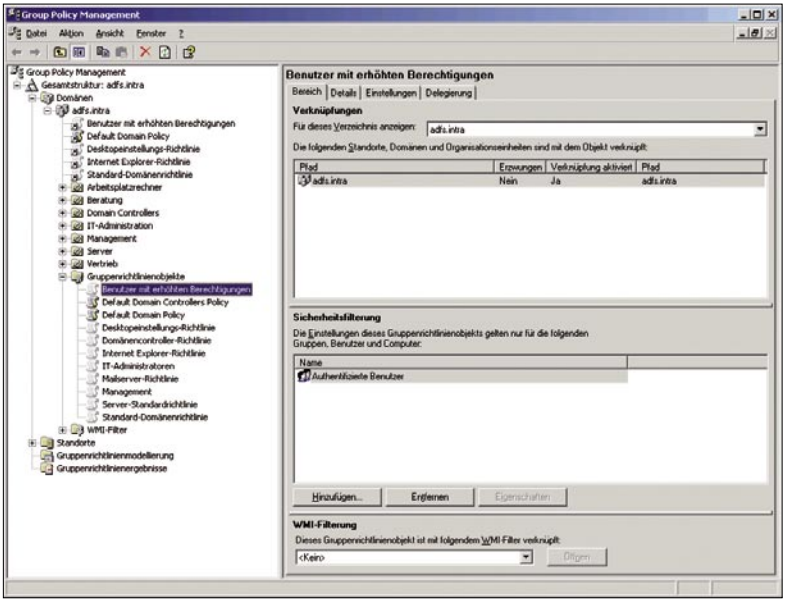
Grundsätzlich gilt, dass man genau planen muss, welche Einstellungen auf welchen Systemen und für welche Benutzer mit welchen Gruppenrichtlinien gesetzt werden sollen. Da es mehrere tausend mögliche Parameter in den Gruppenrichtlinien gibt, ist das ein aufwändiger Prozess. Wenn man sich aber zunächst auf allgemein gültige Einstellungen beschränkt und dort nur die wichtigsten Parameter steuert, kann man schnell erste Erfolge bei der Systemkonfiguration über Gruppenrichtlinien erzielen.

4.2.1 Werkzeuge für das Gruppenrichtlinien-Management

Es gibt sowohl von Microsoft als auch von Drittherstellern etliche Tools, mit denen man Gruppenrichtlinien verwalten kann. Dritthersteller liefern teils Erweiterungen der Funktionalität von Gruppenrichtlinien, teils aber auch Administrationssysteme, in die die Gruppenrichtlinien eingebunden sind. Microsoft selbst

stellt über die Support-Tools und die Resource Kit Tools vor allem Befehlszeilenfunktionen bereit, die für die erweiterte Analyse von Problemen mit Gruppenrichtlinien genutzt werden können.

Für den Einstieg und die meisten Aufgaben im Umgang mit Gruppenrichtlinien gibt es aber nur zwei Werkzeuge, die man benötigt. Das eine ist die *Gruppenrichtlinienverwaltung* oder auch *Group Policy Management Console*, die kurz als GPMC bezeichnet wird. Dabei handelt es sich um ein Add-on, das kostenlos von der Website www.microsoft.com/technet/downloads/winsrvr/featurepacks/default.mspx geladen werden kann – ein so genanntes Feature Pack. Die GPMC ist erst nach der Veröffentlichung des Windows Server 2003 fertig geworden und daher nicht Bestandteil des Betriebssystems.



GPMC: Das wichtigste Werkzeug für die Bearbeitung von Gruppenrichtlinien ist die Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console).

Das zweite Werkzeug ist der *Gruppenrichtlinienobjekt-Editor*. Er kann nach der Installation der GPMC direkt aus dieser aufgerufen werden. Falls man die GPMC nicht nutzt, kann man ihn aus dem Verwaltungsprogramm *Active Directory-Benutzer und -Computer* starten. Aber, kurz gesagt: Es macht überhaupt keinen Sinn, ohne GPMC zu arbeiten, da die GPMC die Administration von Gruppenrichtlinien sehr viel übersichtlicher macht.

4.2.2 Was man über Gruppenrichtlinien unbedingt wissen muss...

Bevor man anfängt, mit Gruppenrichtlinien zu arbeiten, muss man zunächst ein paar grundlegende Dinge wissen. Es sind genau genommen nur drei Punkte, die man aber verinnerlichen muss, um Probleme bei der Nutzung von Gruppenrichtlinien zu minimieren.

- Wie schon der Name des Gruppenrichtlinienobjekt-Editors andeutet, gibt es Gruppenrichtlinienobjekte, die auch kurz als GPOs (Group Policy Objects) bezeichnet werden. Diese Objekte können an verschiedenen Stellen wie bei Domänen und organisatorischen Einheiten verknüpft werden. Damit kann man eine Gruppenrichtlinie mehrfach nutzen. Wenn man das Objekt ändert, wirkt sich das aber auf alle Verknüpfungen aus. Man sollte sich angewöhnen, das Gruppenrichtlinienobjekt grundsätzlich direkt und nicht auf dem Umweg über eine Verknüpfung zu bearbeiten.
- Innerhalb jedes Gruppenrichtlinienobjekts gibt es Einstellungen für Computer und Einstellungen für Benutzer. Erstere gelten für das gesamte System und damit automatisch für alle Benutzer, die sich daran anmelden. Letztere gelten nur für bestimmte Benutzer, dafür aber an allen Rechnern, die von diesen genutzt werden. Die meisten Einstellungen gelten entweder für Computer oder für Benutzer. Einige Parameter lassen sich aber in beiden Bereichen konfigurieren. In diesem Fall muss man sich genau überlegen, an welcher Stelle sie eigentlich richtigerweise gesetzt werden.

4.2.3 Vorsicht vor widersprüchlichen Richtlinien

Der dritte Punkt ist der kritischste und führt in der Praxis oft zu nicht beabsichtigten Effekten. Hierfür sollte man bei der Planung der Richtlinien daher besonders viel Zeit aufwenden:

- Gruppenrichtlinienobjekte können mit verschiedenen Objekten im Active Directory verknüpft werden. Im Einzelnen sind das Standorte, Domänen und organisatorische Einheiten. Die Verarbeitung erfolgt in dieser Reihenfolge. Das bedeutet aber auch, dass Einstellungen aus einer Standort-Richtlinie durch konkurrierende Einstellungen in einer Domänen-Richtlinie überschrieben werden – ebenso wie Einstellungen in der Domänen-Richtlinie durch solche aus organisatorischen Einheiten überschrieben werden können. Die wichtigsten Richtlinien finden sich also sozusagen auf der untersten Ebene von organisatorischen Einheiten. Das Problem lässt sich minimieren, indem man vorher überlegt, welche Richtlinieneinstellung wo gesetzt werden soll. In Einzelfällen wie beispielsweise für Systemadministratoren oder Domänen-Controller kann man dann immer noch übergeordnete Einstellungen auf der Ebene einer organisatorischen Einheit überschreiben. Zur Regel sollte das aber nicht werden.

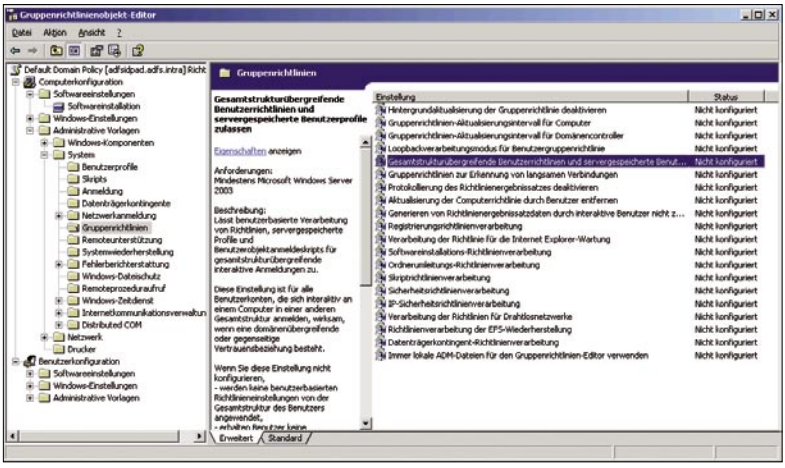
Übrigens lassen sich auch mehrere Richtlinien auf einer Ebene zuordnen. Diese kann man priorisieren. Auch hier ist es aber einfacher, wenn man es vermeidet, dass ein Parameter über mehrere Richtlinien gesetzt wird.

Am letzten Punkt wird zudem deutlich, dass Gruppenrichtlinien das Active Directory voraussetzen. Wenn man nur mit Arbeitsgruppen und ohne Domänen arbeitet, kann man allenfalls lokal einen Ausschnitt der Richtlinien steuern, indem man lokale Sicherheitsrichtlinien konfiguriert.

Natürlich gibt es noch viel mehr wissenswerte Dinge über Gruppenrichtlinien wie beispielsweise Zugriffsberechtigungen, die die Anwendung steuern oder Optionen, um die Vererbung zu unterbrechen. Darauf gehen wir zum Teil in diesem Artikel noch ein. Generell gilt, dass man alles so einfach wie möglich halten sollte, wenn man den Überblick über die Gruppenrichtlinien bewahren will.

4.2.4 Die Standardrichtlinien

Öffnet man die GPMC das erste Mal, finden sich dort zwei Richtlinien. Eine ist als *Default Domain Policy*, die andere als *Default Domain Controllers Policy* bezeichnet. Die Erste ist die Standardrichtlinie für die Domäne, die Zweite enthält nur Parameter für die spezielle Konfigurationsanpassung bei Domänen-Controllern.



Finger weg: Es gibt Standardrichtlinien für Domänen und Domänen-Controller, über die allerdings keine Anpassungen erfolgen sollten – hier die Standardrichtlinie für Domänen im Gruppenrichtlinien-Editor.

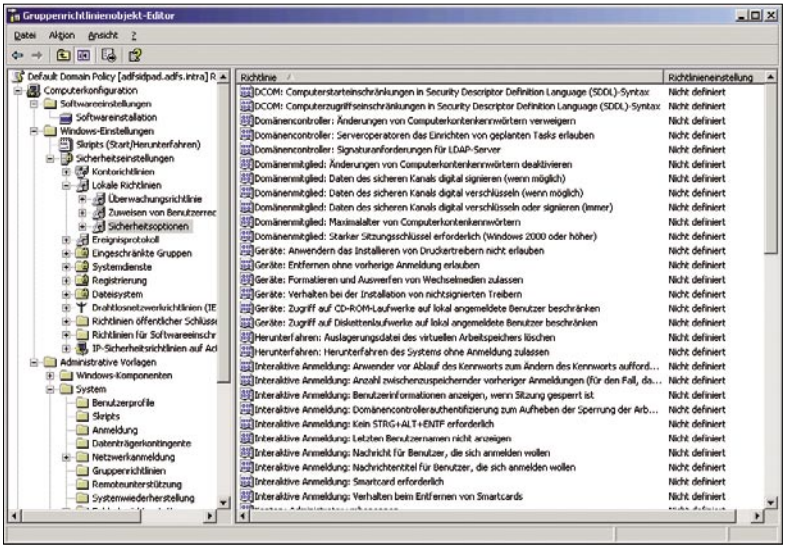
Es ist eine häufig vorzufindende Praxis, dass diese beiden Richtlinien direkt angepasst werden. Das Problem ist, dass Fehler bei diesem Ansatz nur schwer zu korrigieren sind. Es ist sinnvoller, zumindest jeweils eine parallele Richtlinie für die

Anpassungen zu erstellen und auf der gleichen Ebene – also bei der Domäne respektive der *OU Domain Controllers* – zu verknüpfen. Um die Auswirkungen von Änderungen rückgängig zu machen, kann man im schlimmsten Fall diese eigenen, zusätzlichen GPOs löschen. Das ist einfacher als zu versuchen, alle Änderungen in einer der Standardrichtlinien von Hand rückgängig zu machen.

In der Praxis wird man im Laufe der Zeit eine Reihe von Richtlinien entwickeln, mit denen man verschiedene Einstellungen im System steuert. Aber wie ausgeführt: Man kann mit einer Richtlinie für allgemeine Einstellungen in der Domäne beginnen und das Konzept anschließend Schritt für Schritt weiterentwickeln.

4.2.5 Einige interessante Einstellungen

Wie schon erwähnt gibt es einige tausend Einstellungen in den Gruppenrichtlinien. Alleine zwischen dem Service Pack 1 und dem Service Pack 2 für Windows XP wurden beispielsweise mehr als 700 Parameter für die Steuerung des Internet Explorer neu in die Gruppenrichtlinien aufgenommen.

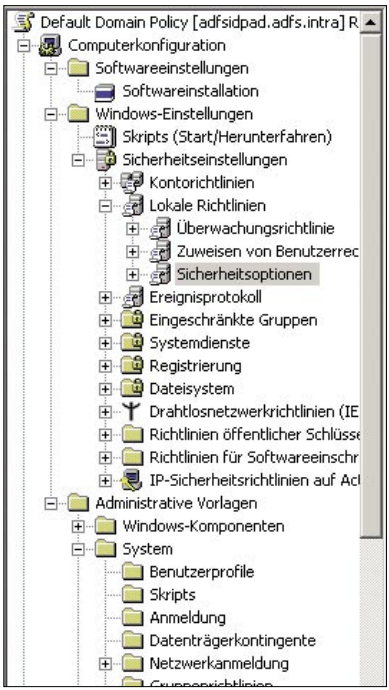


Enges Korsett: Einer der wichtigsten Bereiche in Gruppenrichtlinien sind die Sicherheitsoptionen, mit denen die Handlungsspielräume von Benutzern stark eingeschränkt werden können.

Da es wenig Sinn macht, alle Einstellungen der Reihe nach durchzuarbeiten, nachfolgend als „Appetizer" der Hinweis auf ein paar Bereiche der Gruppenrichtlinien mit besonders interessanten Parametern:

- Im Bereich *Computerkonfiguration – Windows-Einstellungen* gibt es die Sicherheitseinstellungen. Diese gliedern sich wiederum in viele Teilbereiche wie *Lokale Richtlinien – Sicherheitseinstellungen* mit den lokal gültigen Sicherheitseinstellungen. In diesem Bereich der Gruppenrichtlinien werden fast alle wichtigen Konfigurationsparameter für die Sicherheit gesetzt.
- Sowohl bei *Computerkonfiguration* als auch bei *Benutzerkonfiguration* gibt es den Abschnitt *Administrative Vorlagen*. Dort finden sich beispielsweise Einstellungen für den Internet Explorer, mit denen exakt konfiguriert werden kann, wie sich dieser verhält.
- Bei *Benutzerkonfiguration* gibt es unterhalb von *Administrative Vorlagen* den Knoten *Systemsteuerung*. Dort lassen sich unter anderem viele Funktionen der Systemsteuerung für Benutzer deaktivieren.
- Bei *Computerkonfiguration – Administrative Vorlagen – System* ist auch der Bereich Gruppenrichtlinien interessant. Denn dort kann das Verhalten der Gruppenrichtlinien konfiguriert werden.

Das ist nur ein kleiner Ausschnitt der Möglichkeiten, die sich aus den Gruppenrichtlinien ergeben. Es gibt kaum einen Bereich bei Windows-Systemen, der nicht über Gruppenrichtlinien gesteuert werden kann.



Gegliedert: Die Eingabe von Parametern für Gruppenrichtlinien erfolgt in einer hierarchischen Baumstruktur

4.2.6 Gruppenrichtlinien und Systemversionen

Wenn man mit Gruppenrichtlinien arbeitet, muss man sich allerdings einer Tücke bewusst sein: Viele Einstellungen gelten nur für bestimmte Systemversionen. Microsoft hat eigentlich mit jedem Service Pack neue Parameter in die Gruppenrichtlinien aufgenommen. Die meisten Teile von Gruppenrichtlinien werden über so genannte Richtlinienvorlagen gesteuert. Dabei handelt es sich bis Windows XP und Windows Server 2003 um einfache, strukturierte Textdateien. Ab Windows Vista und dem Windows Server Longhorn wird mit XML-Dateien gearbeitet.

Bei der Bearbeitung von Gruppenrichtlinien ist es wichtig, dass man prüft, mit welchen Richtlinienvorlagen man arbeitet. Die neuesten Richtlinienvorlagen sind jeweils auf der Download-Website von Microsoft verfügbar. Da in den Richtlinien Versionsinformationen enthalten sind, halten sich die Probleme in Umgebungen mit unterschiedlichen Windows-Versionen in Grenzen. Man muss aber bei jedem Parameter darauf achten, ob er beispielsweise auch von Windows 2000 unterstützt wird. Wenn man nun beginnen möchte, eigene Gruppenrichtlinien zu erstellen, sollte man zwei Hinweise beachten:

1. Änderungen nur in eigenen, neuen GPOs vornehmen, die man relativ einfach wieder löschen kann.

2. Änderungen in Testumgebungen gründlich austesten, um Probleme in den produktiven Systemen zu vermeiden.

Wenn man sich zusätzlich bei jeder Anpassung noch einmal genau überlegt, welche Konsequenzen diese hat, kann eigentlich nicht mehr viel schiefgehen.

Martin Kuppinger

tecCHANNEL-Links zum Thema	Webcode	Compact
Zentrales Windows-Management durch Gruppenrichtlinien	459881	S.162
Sicherheitsmanagement im Active Directory	460445	S.169
Active Directory in Windows 2003	402162	–
Windows Server 2003 überwachen: Der Systemmonitor	402511	–
Sicherheits-Tuning für Windows Server 2003	402350	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

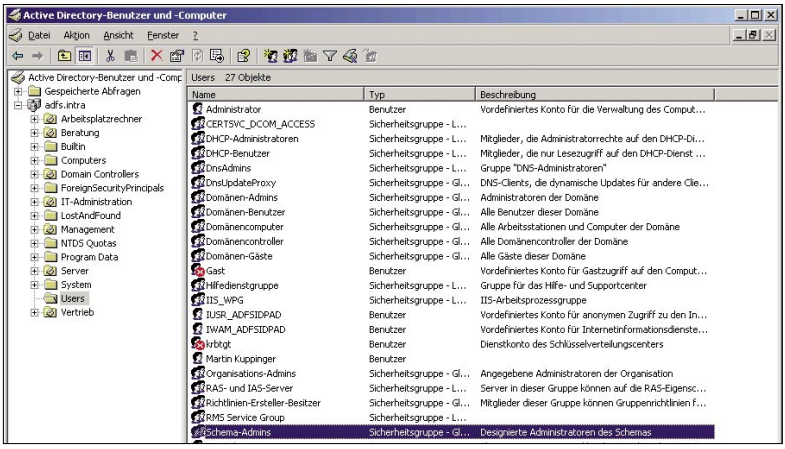
4.3 Sicherheitsmanagement im Active Directory

Das Active Directory ist das zentrale Element der Sicherheitsinfrastruktur in Windows-Umgebungen. Es wird standardmäßig so eingerichtet, dass nur der zunächst definierte Administrator volle Zugriffsberechtigungen hat und Änderungen vornehmen kann. Je größer das Netzwerk wird, desto differenziertere Berechtigungen sind aber erforderlich, um beispielsweise Operatoren nur die Änderung von Benutzerkonten in bestimmten organisatorischen Einheiten zu erlauben oder um ausgewählten Benutzern einzelner Organisationsbereiche die Möglichkeit zu geben, Kennwörter zurückzusetzen.

Wer was im Active Directory machen darf, lässt sich über drei Mechanismen steuern. Der erste und einfachste ist die Zuordnung von Benutzern zu den vordefinierten Gruppen mit spezifischen administrativen Berechtigungen. Der zweite ist die Vergabe von zusätzlichen Berechtigungen über einen Assistenten. Alternativ dazu kann man, als dritte Möglichkeit, die Zugriffsberechtigungen im Active Directory auch direkt bearbeiten.

4.3.1 Vordefinierte Gruppen

Die meisten vordefinierten Gruppen mit administrativen Berechtigungen finden sich im Container Users. In einer Forest-Root-Domäne – also der ersten in einem Forest eingerichteten Domäne – gibt es zunächst drei besonders wichtige administrative Gruppen:



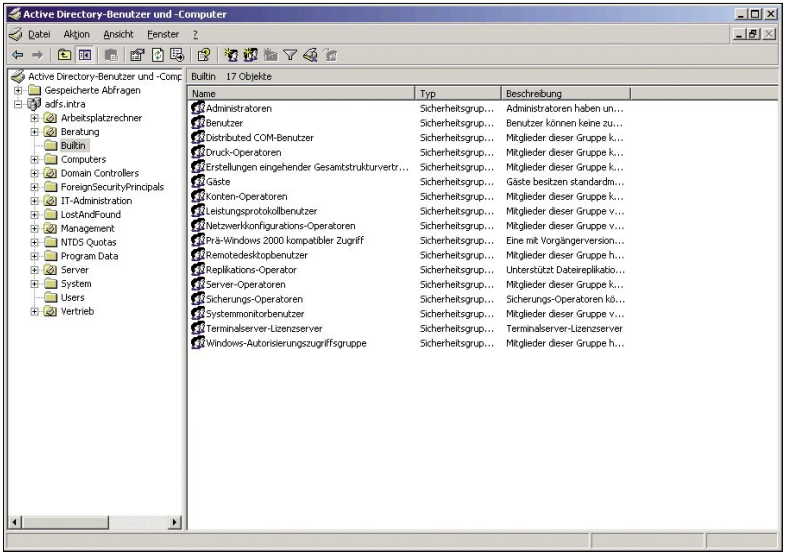
Vorkonfiguriert: Im Container „Users" des Active Directory finden sich vordefinierte Sicherheitsgruppen, die in Sicherheitskonzepten für das Active Directory genutzt werden können.

- Die Gruppe *Domänen-Admins* hat administrative Berechtigungen für die aktuelle Domäne, aber nicht für andere Domänen im Forest. Mitglieder dieser Domäne haben volle Zugriffsberechtigungen und können beispielsweise Benutzer- und Computerobjekte in einer Domäne anlegen.
- Die Gruppe *Organisations-Admins* wird für die Administration der Forest-Struktur benötigt. Die Mitglieder dieser Gruppe dürfen beispielsweise neue Domänen in einem Forest anlegen.
- Die Gruppe *Schema-Admins* hat die Berechtigung zur Änderung des Schemas, also der Datenstruktur des Active Directory.

Grundsätzlich gilt, dass man bei allen Gruppen restriktiv bezüglich der Zuordnung von Nutzern sein sollte, da sie standardmäßig umfassende Rechte besitzen.

4.3.2 Weitere Gruppen

Im Container *Users* finden sich aber auch weitere Gruppen mit administrativen Berechtigungen. Dazu zählen die *DHCP-Administratoren* und *DNS-Admins* mit den administrativen Berechtigungen für diese beiden Infrastrukturdienste und die *Richtlinien-Ersteller-Besitzer*, die Gruppenrichtlinien in einer Domäne modifizieren dürfen. Hier wird schon deutlich, dass durchaus eine Trennung verschiedener administrativer Aufgaben angedacht ist.



Altlasten: Im Container „Builtin" finden sich Operatorengruppen, die aus Gründen der Kompatibilität zu Windows-NT-Domänen definiert wurden. Diese Gruppen können für die Sicherheitsadministration genutzt werden.

Neben dem Container *Users* gibt es auch noch den Container *Builtin* mit vordefinierten Gruppen. Hier gibt es Gruppen wie *Konten-Operatoren* oder *Server-Operatoren*, die bestimmte administrative Aufgaben übernehmen dürfen. Ursprünglich wurden der Container und die darin enthaltenen Gruppen aus Kompatibilitätsgründen zu Windows-NT-Domänen definiert. Sie können aber auch im Active Directory weiter genutzt werden. So hat die Gruppe der *Konten-Operatoren* beispielsweise die Berechtigung zur Verwaltung von Benutzer- und Computerkonten, kann aber keine anderen administrativen Aufgaben übernehmen. Statt eigene operative Gruppen zu erstellen, bietet es sich an, mit diesen vordefinierten Gruppen zu arbeiten.

Dass die Gruppen im Container *Builtin* nicht nur historische Relevanz haben, zeigt sich auch daran, dass es dort spezielle Gruppen für das Active Directory wie die *Erstellungen eingehender Gesamtstrukturvertrauensstellung* gibt. Damit können so genannte Cross-Forest-Trusts erstellt werden, die erst mit dem Windows Server 2003 eingeführt wurden.

Der Vorteil der Nutzung vordefinierter Gruppen liegt darin, dass man die Sicherheitsadministration mit sehr wenig Aufwand durchführen kann. Statt Berechtigungen anzupassen, muss man nur Benutzer oder bereits vorhandene Gruppen in diese speziellen Sicherheitsgruppen aufnehmen.

4.3.3 Die Delegation von Berechtigungen

Ein Nachteil davon, sich auf die genannten vordefinierten Gruppen zu beschränken, liegt darin, dass die zugewiesenen administrativen Berechtigungen dieser Gruppen jeweils für die gesamte Domäne gelten. Wenn man nun aber die Administration einzelner Bereiche einer Domäne bestimmten Benutzergruppen zuordnen möchte, reichen diese Gruppen nicht aus. Gleiches gilt auch, wenn man einer Gruppe zwar das Recht zugestehen möchte, etwa die Telefonnummern und Adressen von Benutzern, die ja auch im Active Directory gespeichert werden können, zu ändern, aber zum Beispiel keine Kennwörter oder Gruppenzuordnungen.

Ein typischer Fall ist die Delegation der Erstellung von neuen Benutzern in einer organisatorischen Einheit an lokale Operatoren. Man kann allerdings auch einzelne Berechtigungen wie das Ändern von Adressdaten oder das Zurücksetzen von Kennwörtern delegieren.

In diesem Fall kommt der *Assistent zum Zuweisen von Objektberechtigungen* ins Spiel, mit dem administrative Berechtigungen delegiert werden können. Der Assistent kann im Kontextmenü von Domänen und organisatorischen Einheiten aufgerufen werden. Dort findet sich jeweils der Befehl *Objektverwaltung zuweisen*.

Im ersten Schritt müssen eine oder mehrere Benutzergruppen ausgewählt werden, denen die neuen Rechte gegeben werden sollen. Man kann zwar theoretisch auch einzelne Benutzer wählen. Davon ist aber unbedingt abzuraten, da es die Administration unübersichtlich und aufwändig macht. Wenn man mit einer Gruppe ar-

beitet, führt man die Zuweisung der Objektberechtigungen einmal durch. Danach kann man sich darauf beschränken, Benutzer in die Gruppe aufzunehmen oder aus der Gruppe zu entfernen.

Würde man dagegen individuelle Benutzer auswählen, dann müsste man bei jeder Änderung dem entsprechenden Benutzer die Berechtigungen wieder manuell entziehen oder sie zusätzlichen Benutzern über den Assistenten geben. Es ist ohnehin eine der „goldenen Regeln" der Windows-Administration, dass man Berechtigungen generell nur an Gruppen vergibt.

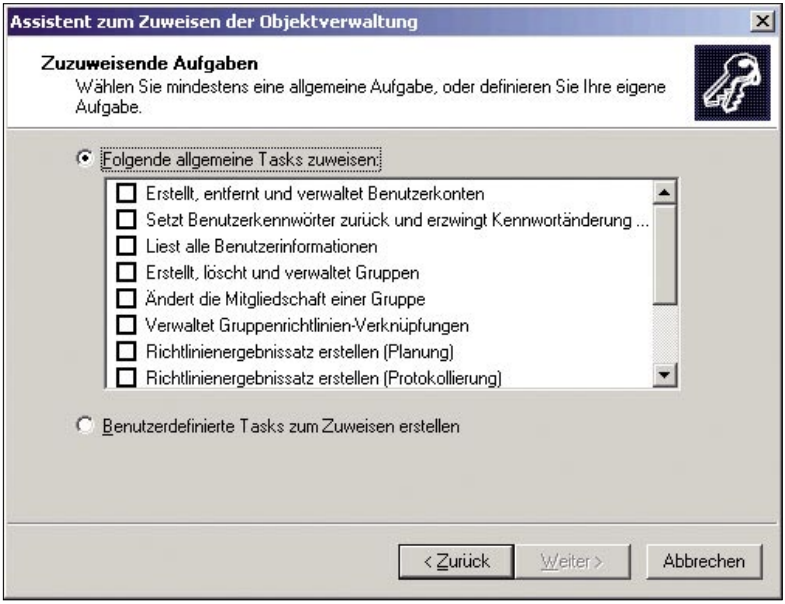
4.3.4 Die vordefinierten Tasks

Der einfachste Ansatz für die Administration ist die Zuweisung vordefinierter Tasks. Eine solche Liste wird bei Nutzung des Assistenten im nächsten Schritt angezeigt. Die Liste unterscheidet sich zwischen Domänen und organisatorischen Einheiten kaum. Bei einer Domäne gibt es die folgenden Tasks:

- Erstellt, entfernt und verwaltet Benutzerkonten
- Setzt Benutzerkennwörter zurück und erzwingt Kennwortänderungen
- Liest alle Benutzerinformationen
- Ändert die Mitgliedschaft einer Gruppe
- Fügt einen Computer einer Domäne hinzu
- Verwaltet Gruppenrichtlinien-Verknüpfungen
- Richtlinienergebnissatz erstellen (Planung)
- Richtlinienergebnissatz erstellen (Protokollierung)
- Erstellt, löscht und verwaltet Konten für inetOrgPerson
- Setzt Kennwörter für inetOrgPerson zurück und erzwingt Kennwortänderungen
- Liest alle Informationen für inetOrgPerson

Bei organisatorischen Einheiten fehlt die Aufgabe *Fügt einen Computer einer Domäne hinzu*. Dafür gibt es die Aufgabe *Erstellt, löscht und verwaltet Gruppen*. Die meisten dieser Aufgaben sind selbsterklärend. Die Richtlinienergebnissätze sind spezielle Analysefunktionen bei Gruppenrichtlinien. In der Planung kann analysiert werden, wie sich eine Gruppenrichtlinie wohl auswirken würde. Bei der Protokollierung kann ermittelt werden, welche tatsächlichen Änderungen durch eine Gruppenrichtlinie verursacht werden.

Die Aufgaben zur *inetOrgPerson* beziehen sich auf spezielle Benutzerobjekte. Die inetOrgPerson ist eine Objektklasse, die in vielen LDAP-Verzeichnissen für Benutzerobjekte verwendet wird. Da es sich dabei um eine zweite Variante von Benutzerkonten handelt, können dafür auch gesondert Zugriffsberechtigungen konfiguriert werden.



Gut gefüllt: Die Liste mit den Aufgaben, die über den Assistenten für die Objektverwaltung bei organisatorischen Einheiten delegiert werden können.

Nach der Auswahl eines oder mehrerer Tasks werden die entsprechenden Berechtigungen vergeben. Abschließend wird ein Dialogfeld angezeigt, in dem man seine Änderungen noch einmal kontrollieren kann.

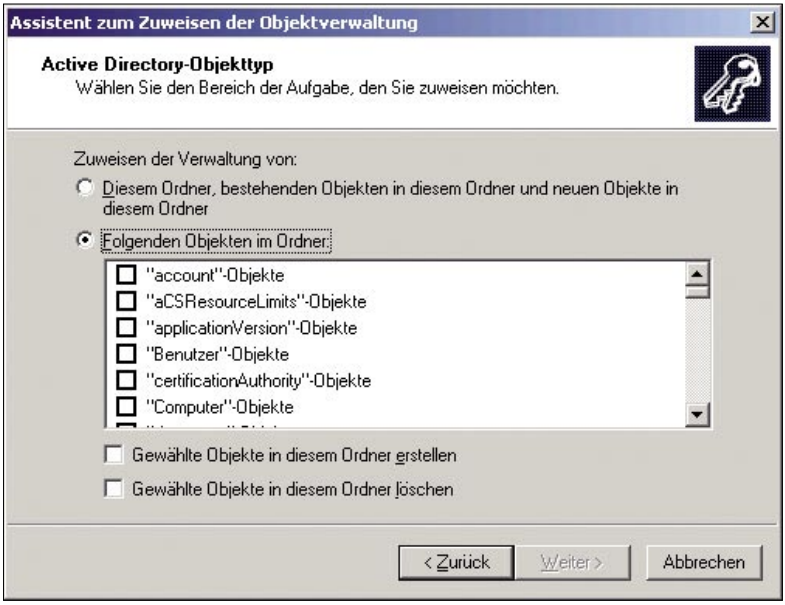
4.3.5 Benutzerdefinierte Tasks

Falls die standardmäßigen Tasks nicht die Anforderungen abdecken, kann man auch eigene Tasks erstellen. Ein Beispiel ist die Erteilung von Änderungsberechtigungen nur für einen Teil der Attribute von Benutzerobjekten, wie sie beispielsweise erforderlich ist, wenn ausgewählte Mitarbeiter in Fachbereichen bestimmte Informationen wie Adressen und Telefonnummern von anderen Mitarbeitern ändern dürfen. Da die Berechtigungen ja unabhängig von der gewählten Schnittstelle gelten, sind solche Anpassungen oft auch für Self-Service-Portale erforderlich.

Mit der Option *Benutzerdefinierte Tasks zum Zuweisen erstellen* lassen sich solche Tasks erzeugen. Die Option findet sich in dem Dialogfeld, in dem oben die allgemeinen (vorgegebenen) Tasks zu sehen sind.

Im nächsten Schritt müssen der oder die Active-Directory-Objekttypen ausgewählt werden, für die Berechtigungen angepasst werden sollen. Eine Option ist die Zuweisung der Berechtigungen für alle Objekte in diesem Ordner und unter-

geordneten Ordnern. In den meisten Fällen sollen die Berechtigungen aber auf bestimmte Objektklassen wie „*Benutzer*“-Objekte beschränkt sein, so dass man entsprechende Objekte auswählen wird. Mit den beiden Optionen *Gewählte Objekte in diesem Ordner erstellen* und *Gewählte Objekte in diesem Ordner löschen* wird gesteuert, ob Objekte auch angelegt und gelöscht oder nur gelesen und geändert werden dürfen.



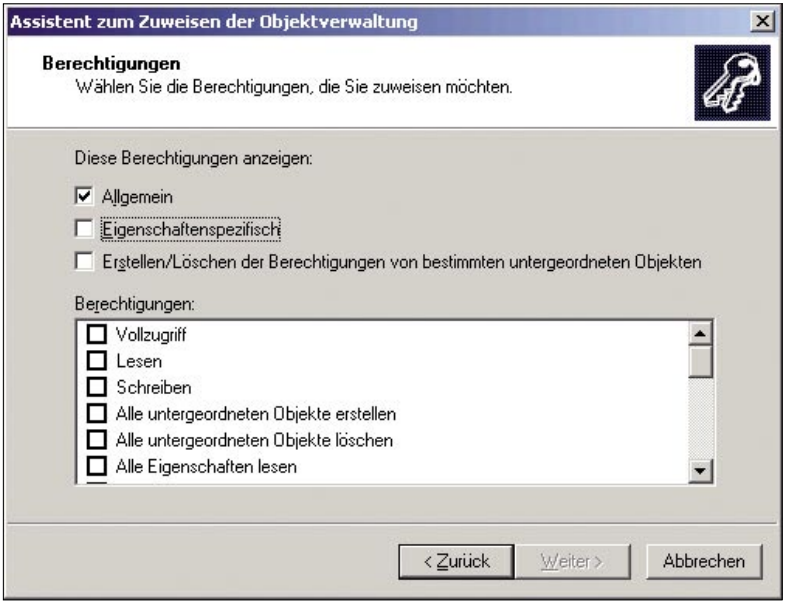
Individuell: Über die Auswahl der Objekte werden eigene Berechtigungen vergeben.

Da es im Active Directory sehr viele Objektklassen gibt, ist die Liste entsprechend lang. Die wichtigsten Objektklassen sind aber einfach identifizierbar, weil sie mit einem Großbuchstaben beginnen. Diese werden vom System sozusagen „erkannt“ und mit einem sprechenden Namen angezeigt, während bei den anderen Objektklassen der generell mit einem Kleinbuchstaben beginnende Name der Objektklasse aus dem Active Directory angezeigt wird.

4.3.6 Die Berechtigungen

Nachdem das oder die Objekte ausgewählt wurden, müssen noch die Berechtigungen konfiguriert werden. Im entsprechenden Dialogfeld des Assistenten werden standardmäßig allgemeine Berechtigungen angezeigt. Dabei handelt es sich um Berechtigungen wie den Vollzugriff, aber auch um vordefinierte, aggregierte

Berechtigungen wie *Kennwort ändern* oder *Lesen und Schreiben Telefon- und Postoptionen*. In vielen Fällen wird man damit auskommen.



Granular: Nach der Auswahl der Objekte müssen die Berechtigungen definiert werden. Diese können bis auf die Ebene einzelner Attribute hinunter gesteuert werden.

Solche aggregierten Berechtigungen finden sich aber nur bei den bereits oben erwähnten Objekten, die vom System speziell behandelt werden. Bei anderen Objekten kann man nur allgemeine Berechtigungen wie beispielsweise *Vollzugriff* setzen oder auf Attributebene steuern, welche Attribute gelesen und welche geändert werden dürfen. Um Berechtigungen auf der Ebene von einzelnen Attributen vergeben zu können, muss man die Option *Eigenschaftenspezifisch* auswählen. Danach wird die vollständige Liste aller Attribute angezeigt. Jedes Attribut erscheint in der Auflistung zweimal, einmal in der Form *accountExpires lesen* und einmal in der Art von *accountExpires schreiben*.

Von der Vergabe von Berechtigungen auf Attributebene ist grundsätzlich eher abzuraten. Das Problem dabei ist, dass man schnell den Überblick verliert. Solange man mit den vordefinierten Aufgaben oder mit den genannten aggregierten Berechtigungen auskommt, sollte man diese nutzen. Falls sie nicht reichen, muss man natürlich auf der Ebene einzelner Eigenschaften arbeiten. Spätestens dann gilt aber auch, dass man jede Zuweisung von Objektrechten ganz genau dokumentieren sollte, um auch nach einiger Zeit noch nachvollziehen zu können, wer welche Berechtigungen im Active Directory hat.

4.3.7 Standorte und Dienste

Berechtigungen lassen sich übrigens nicht nur für Domänen und organisatorische Einheiten über den Assistenten setzen, sondern auch für Standorte, Dienste und die Kommunikation zwischen Standorten (Inter-Site Transports). Im Verwaltungsprogramm *Active Directory-Standorte und -Dienste* findet sich im Kontextmenü ebenfalls jeweils der Befehl *Objektverwaltung* zuweisen.

Allerdings beschränkt sich die Konfiguration hier in der Praxis darauf, dass man einerseits einer ausgewählten Operatorengruppe die Standort- und Transportverwaltung zuweist und andererseits einer Gruppe die Dienstverwaltung. Mehr Anpassungen sind hier normalerweise nicht erforderlich. Allenfalls in sehr großen Infrastrukturen könnte eine regionale Trennung noch Sinn machen.

Mit dem Assistenten für die Zuweisung der Objektverwaltung lassen sich aber in erfreulich einfacher Weise Berechtigungen im Active Directory setzen und damit Benutzergruppen Zugriffsrechte zuordnen. In der englischen Version wird auch von Delegation gesprochen – und genau darum geht es: Die gezielte Delegation gewählter Verwaltungsaufgaben an spezielle Gruppen im Active Directory. Denn diese gezielte und beschränkte Delegation ist die Basis für die Sicherheit des Active Directory. Wenn viele alles oder zumindest sehr viel dürfen, ist diese nicht zu gewährleisten – bei einer gezielten, eingeschränkten Delegation dagegen schon.

Martin Kuppinger

tecCHANNEL-Links zum Thema	Webcode	Compact
Sicherheitsmanagement im Active Directory	460445	S.169
Zentrales Windows-Management durch Gruppenrichtlinien	459881	S.162
Active Directory: Unentbehrliche Helfer für Admins	443285	–
Katastrophenszenarien bei Active Directory	434994	–
Active Directory in Windows 2003	402162	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

5. Notes / Domino Inside

Die Lotus-Domino-Serverarchitektur bildet das Rückrat von IBMs dokumentenorientierter Kollaborationssoftware, auf die Clients mit Lotus Notes zugreifen. Eine anspruchsvolle Aufgabe ist die Administration der integrierten Public-Key-Infrastruktur. In diesem Kapitel lesen Sie, wie Sie Server-basierte Zertifikate in den Griff bekommen. Außerdem erklären wir die Möglichkeiten der Serverüberwachung mit Domino Domain Monitoring. Ein weiterer Workshop zeigt, wie Sie Domino und Outlook zu einem effektiven Gespann kombinieren.

5.1 Domino: Der Server-basierte Zertifikatsdienst

Lotus Domino nutzt digitale Zertifikate schon immer für die Sicherheit – bei der Authentifizierung, der Kommunikation zwischen Systemen und der Speicherung von Daten. Ab der Version 6 gibt es mit der Server-basierenden CA einen neuen Zertifikatsdienst, der sowohl für das Management von Notes- als auch Internet-Zertifikaten genutzt werden kann.

Im Notes/Domino-Umfeld werden zwei Varianten von Zertifikaten genutzt. Zum einen sind das die Notes-Zertifikate, die für die systeminterne Kommunikation verwendet werden, zum anderen die Internet-Zertifikate, die beispielsweise für SSL oder S/MIME genutzt werden. Letztere entsprechen dem Standard X.509v3, während die Notes-Zertifikate sich davon unterscheiden.

Da schon für die internen Aufgaben Zertifikate erforderlich sind, wird auch ein Zertifikatsdienst benötigt, bei Lotus ist das die Certification Authority oder CA. Bis zur Version 5.x gab es dabei eine zwingende Trennung zwischen der integrierten, automatischen Erstellung von Notes-Zertifikaten und einer optionalen, getrennten CA für die Erstellung von Internet-Zertifikaten. Ab der Version 6.0 kann dagegen mit der Server-basierenden CA gearbeitet werden, die beide Funktionen integriert. Die bisherigen Ansätze können aber weiterhin verwendet werden. Die erstellten Zertifikate sind miteinander kompatibel. Es geht also „nur“ um eine administrative Änderung.

5.1.1 Basis der Zertifikate

Die Basis für die Änderungen bildet der CA-Prozess. Dabei handelt es sich um einen Server-Prozess von Domino, der auf ausgewählten Systemen zusätzlich als Task gestartet werden muss. Neben dem wichtigen Punkt, dass sich Zertifikate nun über eine einheitliche Schnittstelle administrieren lassen, ist die entscheidende Änderung aber, dass die Erstellung von Zertifikaten keine Kenntnis des Kenn-

worts des so genannten Zertifizierers mehr benötigt, sondern dass mit zu Benutzerkonten zugeordneten Rollen gearbeitet wird. Der Zertifizierer ist das Zertifikat der Stelle, die Zertifikate erzeugt, beispielsweise einer organisatorischen Einheit innerhalb einer Notes-Infrastruktur. In der Regel ist er in einer Datei *cert.id* gespeichert. Die Nutzung einer solchen Datei über ein mehreren Benutzern bekanntes Kennwort ist nicht sonderlich sicher. Bei der Server-basierenden CA erfolgt dagegen die Authentifizierung mit der jeweils persönlichen Notes-ID, der die entsprechende Rolle eines RAs (Registration Agent) zugeordnet ist.

Darüber hinaus gibt es noch eine Reihe anderer wichtiger Erweiterungen. So werden nun CRLs (Certificate Revocation Lists) mit Informationen zu nicht mehr gültigen Zertifikaten und ICLs (Issued Certificate Lists) mit Daten über die ausgegebenen Zertifikate unterstützt.

5.1.2 Die Grundkonfiguration

Um mit dem CA-Prozess arbeiten zu können, sind mehrere Schritte erforderlich:

1. Der CA-Prozess muss gestartet werden. Dazu wird der entsprechende Task geladen. Der Status kann mit *tell ca stat* überprüft werden.

2. Mindestens ein vorhandener Zertifizierer muss für den CA-Prozess migriert werden.

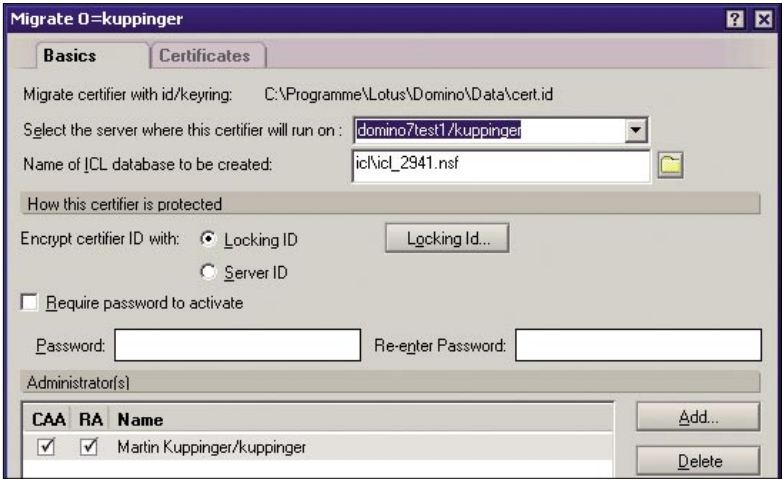
3. Die zuständigen Administratoren müssen festgelegt werden.

Der erste Schritt ist einfach, da es sich um die normale Vorgehensweise beim Start eines Tasks handelt. Um den Zertifizierer zu migrieren, wird im Domino Administrator im Register *Configuration* bei *Tools* der Befehl *Certification – Migrate Certifier* verwendet. Dort muss zunächst über Select die Datei mit dem Zertifizierer gewählt werden. Standardmäßig ist das die Datei *cert.id* im Verzeichnis *domino\data*. Für diese Datei muss das Kennwort angegeben werden.

Im angezeigten Dialogfeld müssen zunächst der Server mit dem CA-Prozess und der Name der ICL-Datenbank angegeben werden. Die ICL-Datenbank wird standardmäßig mit einem automatisch generierten Dateinamen angelegt.

Darunter muss definiert werden, wie der Zertifizierer geschützt werden soll. Hier gibt es zwei Optionen. Die Verwendung der Server-ID bietet relativ wenig Schutz, solange ohne Kennwort gearbeitet wird. Bei Nutzung eines Kennworts ist das Problem aber, dass dieses wieder mehreren Personen bekannt sein muss. Besser ist eine Locking-ID, die an ein gegebenenfalls auch speziell für diesen Zweck erstelltes Benutzerkonto gekoppelt ist.

Im unteren Bereich können die Administratoren konfiguriert werden. CAAs (Certificate Authority Administrators) sollte es wenige geben. Diese dürfen grundlegende Einstellungen der CA anpassen. RAs (Registration Agents) kann es dagegen mehr geben, weil diese beim Anlegen von Benutzern die erforderlichen Zertifikate über die CAs anfordern dürfen.



Basisdaten: Um die Server-basierende CA nutzen zu können, müssen be-stehende Zertifizierer zunächst migriert und die Administratoren definiert werden.

5.1.3 Einstellungen zu Zertifikaten

Der nächste Konfigurationsschritt ist die Festlegung der Einstellungen zu Zertifikaten. Im Register *Certificates* kann festgelegt werden, welche Lebensdauer *EE-Certificates* (End Entities, also die Benutzer und Systeme, für die Zertifikate ausgestellt werden) und das *CA Certificate* haben. Die Einstellungen können bei der Ausgabe von Zertifikaten im definierten Wertebereich angepasst werden. Die gewählten Werte sind relativ hoch und lassen sich aus Sicherheitsgründen verkürzen. Die Änderung wird als administrative Anforderung an den Admin-Prozess (adminp) übergeben. Statt darauf zu warten, dass sie im Rahmen der turnusmäßigen Verarbeitung durchgeführt wird, kann man mit

```
tell adminp process all
```

eine sofortige Verarbeitung veranlassen. Das kann jedoch dazu führen, dass auch andere und mitunter lastintensive Verarbeitungsschritte ausgelöst werden. Mit

```
tell ca refresh
```

kann anschließend dafür gesorgt werden, dass die Einstellungen der CA aktualisiert werden. Das Ergebnis lässt sich mit

```
tell ca stat
```

betrachten. Hier wird angegeben, welche Zertifizierer bereits migriert wurden und damit im Rahmen des CA-Prozesses nutzbar sind.

Ab diesem Zeitpunkt kann der CA-Prozess bei der Registrierung von Benutzern verwendet werden. Bei der Auswahl des Zertifizierers muss man nun nicht mehr die Datei angeben, sondern kann den CA-Prozess und dort den gewünschten Zertifizierer auswählen.

Einfacher nutzbar: Bei Verwendung des CA-Prozesses wird kein Kennwort für eine Zertifizierer-ID mehr benötigt. Ein RA kann den gewünschten Zertifizierer beim Anlegen von Benutzern einfach auswählen.

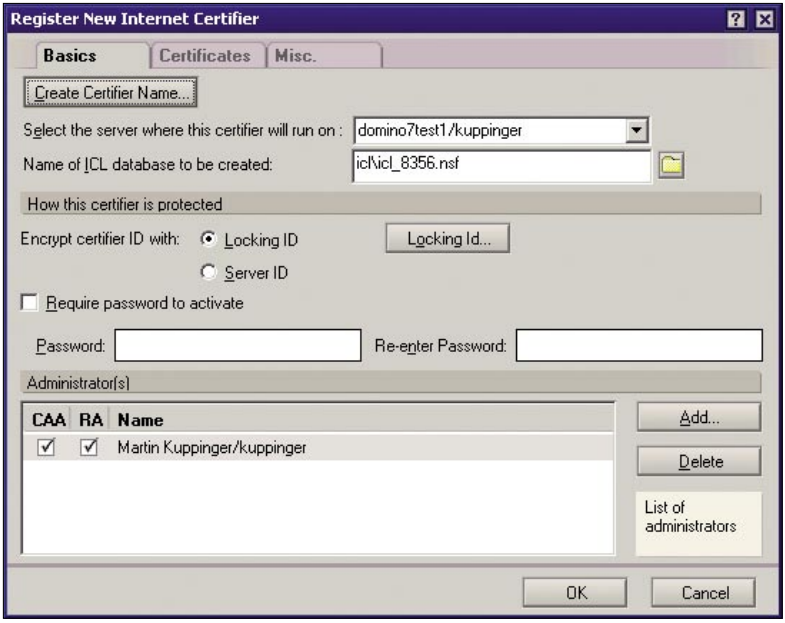
5.1.4 Internet-Zertifikate

Neben den Notes-Zertifikaten lassen sich auch Internet-Zertifikate erstellen. Dafür wird entweder die Keyring-Datei einer bestehenden CA benötigt oder es wird ein neuer Zertifizierer erstellt, der von dem eigenen Zertifikatsdienst verwendet wird. In diesem Fall muss man später die CA des CA-Prozesses noch als vertrauenswürdige Stammzertifizierungsstelle bei den Clients konfigurieren.

Ein Internet-Zertifizierer für den CA-Prozess wird ebenfalls im Bereich *Configuration* des Domino Administrator erstellt. Bei *Tools* gibt es den Befehl *Registration – Internet Certifier*. Im angezeigten Dialogfeld kann zwischen der Keyring-Datei und einem neuen Zertifizierer gewählt werden.

Wenn ein neuer Zertifizierer angelegt wird – also faktisch das Zertifikat für die Stammzertifizierungsstelle, die der CA-Prozess zukünftig darstellen soll – wird ein Dialogfeld angezeigt, das auf den ersten Blick weitgehend dem entspricht, das

auch bei Notes-Zertifizierern verwendet wird. Im oberen Bereich gibt es aber eine zusätzliche Schaltfläche *Create Certifier Name*. Dort müssen die Standardinformationen zu einer CA wie der *Common Name* als identifizierender, eindeutiger Name und die organisatorische Einheit angegeben werden.



Wichtig: Für Internet-Zertifikate müssen bei der Einrichtung der CA die Einsatzbereiche der Zertifikate explizit angegeben werden.

Das Register Certificates

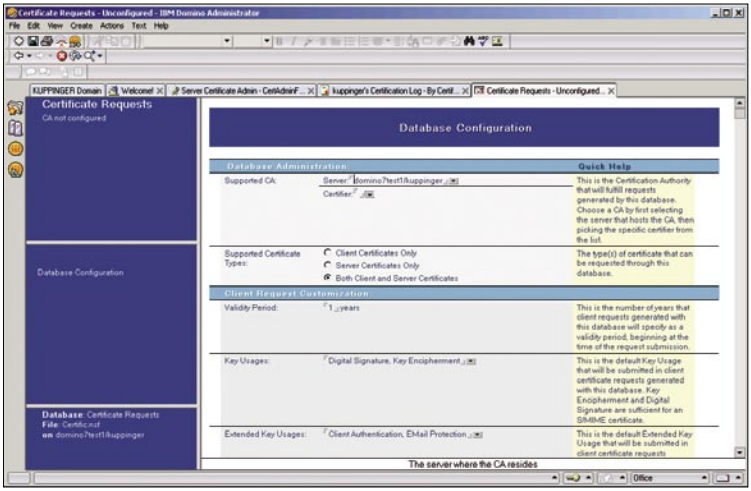
Wesentlich mehr Unterschiede gibt es im Register *Certificates*. In diesem können im oberen Bereich Informationen zu den CRLs und darunter Festlegungen zur Schlüsselnutzung getroffen werden. Dabei gibt es mögliche Einsatzbereiche für Zertifikate und solche, die in jedem Fall erlaubt sind. Man muss hier genau überlegen, welche der Einsatzbereiche erforderlich sind.

Schließlich gibt es noch das Register *Misc*. In diesem werden ergänzende Informationen wie der verwendete Algorithmus für Signaturen, das Ablaufdatum für das Zertifikat oder die Lebensdauer der CRL konfiguriert.

Zu beachten sind noch zwei weitere Punkte:

1. Zertifizierer können nur bearbeitet werden, wenn der CA-Prozess nicht läuft. Das setzt eine genaue Planung der administrativen Tätigkeiten voraus.

2. Zertifizierer müssen bei der ersten Nutzung und teilweise nach Aktualisierungen an der CA oder einem Neustart des CA-Prozesses aktiviert werden. Dazu wird bei Verwendung der Server-ID für die Verschlüsselung der Befehl `tell ca activate` mit der Nummer des Zertifizierers und gegebenenfalls dem Kennwort verwendet. Bei Benutzung einer Locking-ID wird dagegen mit `tell ca unlock` mit der ID-Datei und dem Kennwort als Parameter gearbeitet.



Schnittstelle: Über die Certificate-Requests-Datenbank können Internet-Zertifikate vom CA-Prozess angefordert und die Anforderungen bearbeitet werden.

5.1.5 Weitere Funktionen

Der CA-Prozess verfügt über eine Reihe von wichtigen Schnittstellen für die weitere Administration:

- Die *Certificate Requests*-Datenbank, die auf Basis der Vorlage *certreg.ntf* erstellt wird, wird für die Verwaltung von Zertifikatsanforderungen verwendet. Außerdem können Benutzer über die Webschnittstelle auch Internet-Zertifikate anfordern.
- Die *Administration Requests*-Datenbank gibt es standardmäßig. In ihr werden administrative Anforderungen gespeichert, die von AdminP verarbeitet werden. Die Bestätigung von Zertifikatsanforderungen erfolgt in dieser Datenbank, nachdem sie manuell oder automatisch aus der Certificate-Requests-Datenbank übergeben wurden.
- Die Datenbanken mit den Certificate Revocation Lists (CRLs) werden genutzt, um Informationen über gesperrte Zertifikate bereitzustellen. Die Informationen werden aber in der ICL-Datenbank (Issued Certificates List) abgelegt.

- Die ICL-Datenbank wiederum ist auch von Bedeutung, um einen Überblick über alle ausgestellten Zertifikate zu erhalten.

5.1.6 Fazit

Da zusätzlich auch noch der Domino Administrator für die Verwaltung benötigt wird, sind das ziemlich viele Schnittstellen, die man kennen muss. Wenn man den CA-Prozess aber erst einmal eingerichtet hat, relativiert sich das. Dann werden Benutzer im Domino Administrator registriert und Zertifikatsanforderungen im Zusammenspiel der Certificate-Requests- und der Administration-Requests-Datenbank bearbeitet. Die anderen Datenbanken benötigt man nur in Ausnahmefällen oder um sich einen Überblick über den Status zu verschaffen.

In jedem Fall gilt: Mit dem CA-Prozess wird die Verwaltung sowohl von Notes- als auch von Internet-Zertifikaten in Domino-Infrastrukturen deutlich einfacher. Deshalb macht der Schritt Sinn, auch wenn man mit dem bisherigen Modell gut vertraut ist und dieses weiterhin unterstützt wird.

Martin Kuppinger

tecCHANNEL-Links zum Thema	Webcode	Compact
Domino: Der Server-basierte Zertifikatsdienst	460940	S.177
Domino Domain Monitoring richtig nutzen	460446	S.184
DAMO: Outlook und IBM Domino – elegant kombiniert	460009	S.190

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

5.2 Domino Domain Monitoring richtig nutzen

Mit dem Domino Domain Monitoring hat Lotus seit der Version 7 eine wichtige Erweiterung realisiert, mit der sich auch mehrere Server besser überwachen lassen. Das DDM ist für Domino-Administratoren kein völliges Neuland. Die Basis bilden die bisherigen Monitoring-Funktionen, die über die *Monitoring Configuration*-Datenbank (events4.nsf) konfiguriert werden können. Die wesentliche Erweiterung liegt darin, dass sich nun viel besser als bisher Informationen von verschiedenen Domino-Servern konsolidieren lassen. Damit verschafft sich der Administrator einen schnellen, zentralen Überblick über Probleme auf verschiedenen Servern. Im Rahmen dieses Workshops zeigen wir Ihnen, wie Sie die Monitoring-Funktion von Domino effizient und sinnvoll einsetzen.

5.2.1 Probes und Monitoring

Für das Verständnis von DDM ist der Begriff der Probes von zentraler Bedeutung. Probes sind Analysen, mit denen definierte Fehlersituationen und Verhaltensweisen eines oder mehrerer Server überprüft werden. Es gibt viele vordefinierte Probes, zusätzlich aber die Möglichkeit, auch eigene Probes zu erstellen.

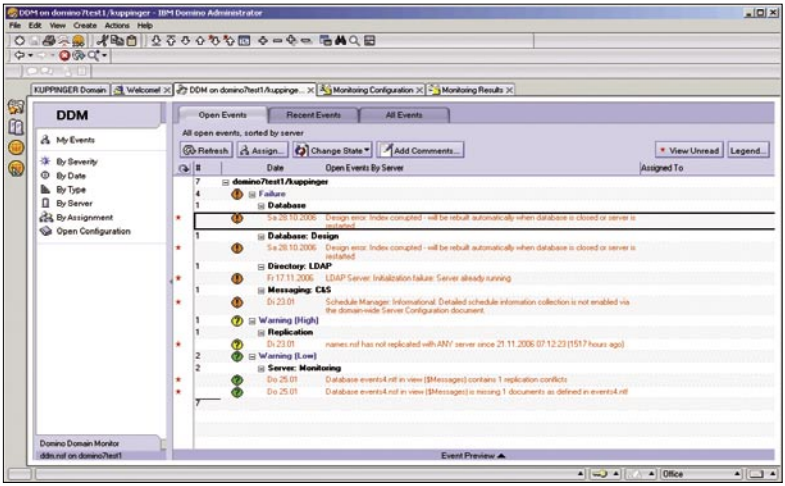
Dadurch, dass das DDM eng mit anderen Überwachungsfunktionen integriert ist, kann man auch keine isolierte Betrachtung nur dieser Funktionalität vornehmen. Viele der Funktionen gibt es auch für das Management einzelner Server.

Für die Nutzung von DDM und den zugrunde liegenden Überwachungsfunktionen gibt es mehrere wichtige Datenbanken und Schnittstellen:

- Im Domino Administrator finden sich Informationen über Ereignisse, die auf einem Server protokolliert wurden, im Bereich *Analysis* und dort unterhalb von *Events*.
- Die Konfiguration wichtiger Einstellungen zum Monitoring kann im Bereich *Configuration* des Domino Administrator erfolgen. Dort gibt es den Abschnitt *Monitoring Configuration*, in dem unter anderem DDM-Filter und DDM-Probes definiert werden können.
- Die Schnittstelle für das Management von DDM-Ereignissen ist die DDM-Datenbank. Dort können Ereignisse, beispielsweise zur Bearbeitung, einzelnen Administratoren zugewiesen werden, so dass sich nachvollziehen lässt, welche Probleme gelöst sind und welche noch nicht.
- Die Konfiguration kann alternativ zum Domino Administrator auch über die bereits erwähnte *Monitoring Configuration*-Datenbank erfolgen.
- Einen Überblick über alle protokollierten Ereignisse liefert die *Monitoring Results*-Datenbank.

5.2.2 Der Umgang mit Ereignissen

Schon in der Standardkonfiguration von DDM werden einige Probes durchgeführt und entsprechend potenziell auch Fehlersituationen protokolliert. In der DDM-Datenbank kann man auf diese zugreifen. Alle protokollierten Fehler und Warnungen sind mit einem Datum und einer beschreibenden Nachricht versehen. Diese Nachricht hilft häufig bereits dabei, das Problem zu lösen oder gibt zumindest gute Hinweise, um die Ursache für die generierte Meldung zu suchen.



Überblick: Die von DDM erfassten Fehler und Warnungen werden übersichtlich in der DDM-Datenbank angezeigt und können dort Administratoren zur Bearbeitung zugeordnet werden.

Zunächst einmal ist es grundsätzlich empfehlenswert, mit DDM zu arbeiten, um Domino-Infrastrukturen zu überwachen, Fehler zu erkennen und diese gezielt und strukturiert abzuarbeiten. Das setzt aber auch voraus, dass man klare Regeln und Verantwortlichkeiten für diese Abarbeitung von erkannten Problemsituationen definiert, also insbesondere die Funktionen für die Zuweisung von Ereignissen zu bestimmten Administratoren nutzt.

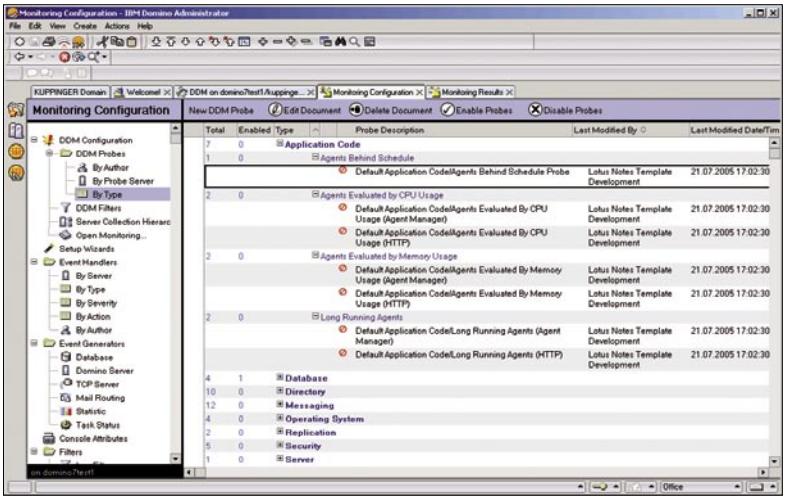
Die Schaltflächen im Detail

Falls man mehr Server und größere Listen hat, kann man diese über die Auswahloptionen auf der linken Seite nach Bedarf strukturieren. Noch wichtiger sind aber die Schaltflächen im oberen Bereich. Mit *Assign* kann man dort eine Zuordnung eines Ereignisses zu einem Benutzer vornehmen. Man kann also klar regeln, wer für die Lösung welches technischen Problems verantwortlich ist. Über die Auswahl von *By Assignment* auf der linken Seite kann man später schnell prüfen, wer welche Ereignisse noch nicht bearbeitet hat.

Mit *Comment* lassen sich ergänzende Kommentare definieren, um etwa die Problemlösung direkt zu dokumentieren oder Hinweise für die Lösung bei einem Ereignis zu hinterlegen. Da man auf eine Liste aller Ereignisse zugreifen kann, wird die DDM-Datenbank so auch zu einer „Knowledge Base“ mit gespeicherten Erfahrungen zur Fehlerbehebung. Mit *Change State* kann ein Eintrag schließlich als gelöst bezeichnet werden. Er ist dann nur noch bei *All Events* zu sehen.

5.2.3 DDM Probes

Die Menge der erfassten Ereignisse beim DDM hängt davon ab, welche Probes definiert und aktiviert sind. Es gibt etliche vorkonfigurierte Probes, die man nutzen kann. Die Bearbeitung erfolgt am besten in der *Monitoring Configuration*-Datenbank. Dort kann man sich die vorkonfigurierten Probes anschauen.

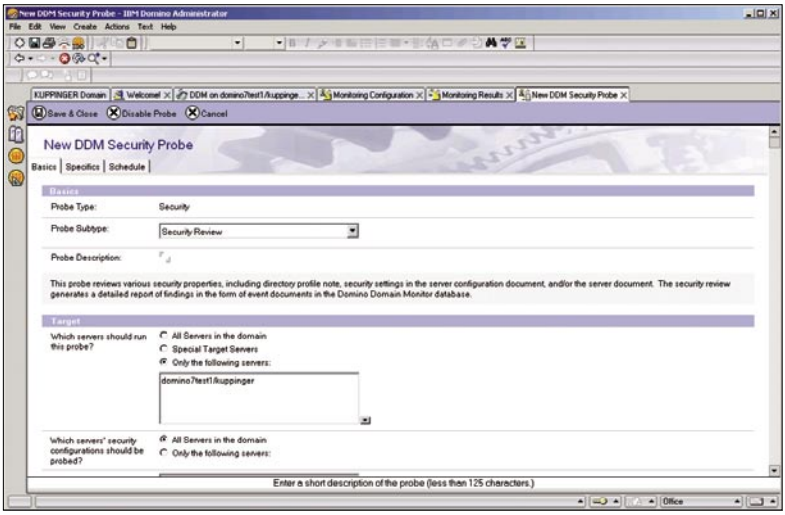


Vordefiniert: Viele DDM-Probes sind bereits vordefiniert. Allerdings sind die meisten davon nicht aktiv und liefern daher keine Daten.

Auch hier finden sich wieder mehrere Ansichten mit einer unterschiedlichen Strukturierung der Informationen. Die Ansicht *By Type* ist für den Einstieg am besten geeignet, da die Probes dort nach ihrer Funktionalität geordnet sind. Wenn man die Probes betrachtet, wird deutlich, dass die meisten Probes als deaktiviert markiert sind. Diese müssen also manuell aktiviert sein. Dazu wird die Schaltfläche *Enable Probes* oberhalb der Liste verwendet. Gut erkennbar ist in dieser Liste auch, ob es schon selbst erstellte Probes gibt. Alle standardmäßig definierten Probes haben als Autor *Lotus Notes Template Development*. Bei eigenen Probes wird dagegen der jeweilige Benutzername als Autor angezeigt.

5.2.4 Gezielte Analyse statt Unmengen von Daten

Bevor man nun in Masse Probes aktiviert, sollte man zunächst einerseits überprüfen, welche Funktion diese überhaupt haben und anschließend überlegen, ob man sie wirklich benötigt. Immerhin verursacht jede Probe auch zusätzliche Last im System, so dass es keineswegs Sinn macht, alle Probes zu aktivieren. Details zu den Probes erhält man, wenn man das jeweilige Probe-Dokument durch einen Doppelklick öffnet. Bei jeder vordefinierten Probe finden sich umfassende Informationen zu der Funktion.



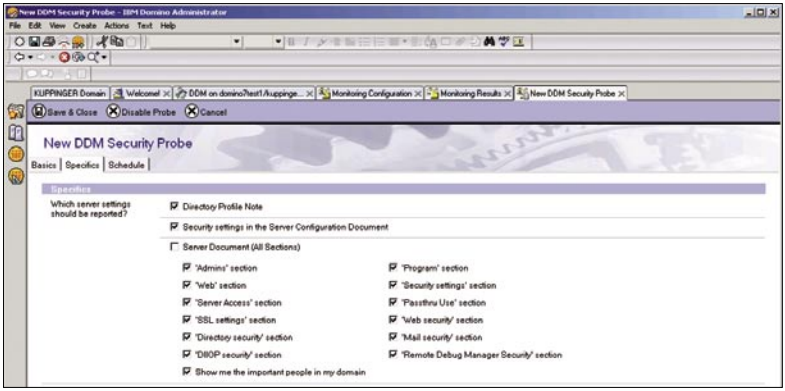
Nicht zu viel: Statt alle Situationen zu überprüfen, sollte man bei jeder Probe überlegen, welche Probleme man erfassen muss und welche nicht relevant für die eigene Infrastruktur sind. Denn Probes verursachen auch Last.

Auch wenn eine Probe vielleicht auf einem Server sinnvoll ist, heißt das noch lange nicht, dass sie generell eingesetzt werden sollte. Man muss also zudem die Liste der Server überprüfen. Und wenn man schon dabei ist, sollte man gleich analysieren, ob alle Detailfunktionen von Probes benötigt werden. Häufig lassen sich einzelne Events auch deaktivieren.

5.2.5 Eigene Probes erstellen

Die Details kann man natürlich bei der Erstellung eigener Probes modifizieren, neue legen Sie mit *New DDM Probe* an. Im ersten Schritt muss man eine der neun vordefinierten Kategorien wie *Database* oder *Security* auswählen. Für jede Kate-

gorie gibt es wiederum *Subtypes*, also untergeordnete, vorkonfigurierte Typen. Das Erstellen eigener Typen ist nicht möglich, Sie sind auf die von Lotus definierten Typen und Subtypen angewiesen.



Anpassbar: Man kann eigene DDM-Probes erstellen und diese gezielt Servern zuordnen.

Im Register *Basics* kann neben der Festlegung des Subtyps eine Beschreibung eingegeben werden. Außerdem wird dort das Ziel der Probe definiert, also die Server, auf denen die Probe ausgeführt werden soll und die Server, die überprüft werden sollen. Ein Server kann also auch Analysen auf anderen Servern durchführen. Dieser Konfigurationsschritt ist einer der wichtigsten, weil man damit die durch das Monitoring erzeugte Last maßgeblich beeinflusst. Während beispielsweise Sicherheitsanalysen auf allen Servern erfolgen sollten, sind andere Bereiche wie *Directory* oder *Web* nur für die Server relevant, auf denen die entsprechenden Tasks ausgeführt werden.

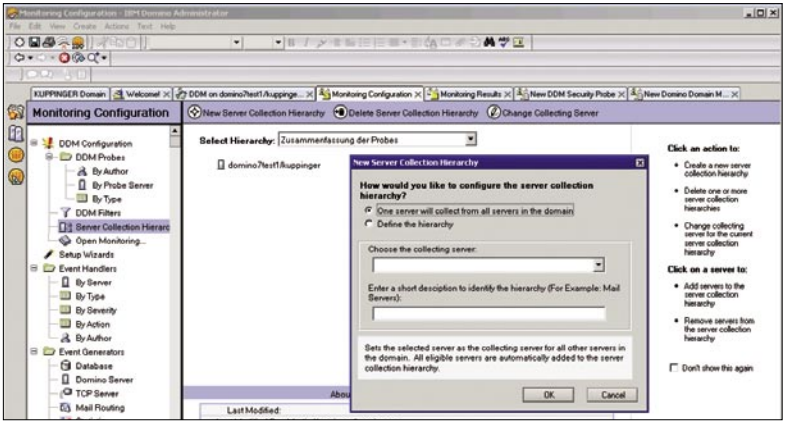
Weitere Einstellungen finden sich im Register *Specifics*. Dort kann man gezielt auswählen, welche Teilanalysen ausgeführt werden sollen. Falls für verschiedene Server verschiedene Teilbereiche getestet werden sollen, kann man auch mehrere Probes erstellen, in denen unterschiedliche Festlegungen in diesem Register getroffen werden. Zudem kann im Register *Schedule* noch ein Zeitplan für die Ausführung von Probes konfiguriert werden. Hier gilt es wieder, einen Kompromiss zwischen Aktualität und umfassender Erkennung von Problemen auf der einen Seite und der durch Probes entstehenden Last auf der anderen Seite zu finden.

5.2.6 Hierarchien und Filter

Wichtig beim DDM sind auch die Hierarchien und Filter. Letztere sind einfach zu erklären: Ein Filter legt fest, welche Ereignisse verarbeitet werden sollen. Damit kann gesteuert werden, dass beispielsweise weniger kritische Ereignisse nicht

übernommen werden. Das ist vor allem in komplexeren Infrastrukturen von Bedeutung, in denen Ereignisse von Dutzenden oder Hunderten von Servern eingesammelt werden, um eine Überfrachtung mit Detaildaten zu verhindern.

Die Hierarchien steuern dagegen, wie Daten gesammelt werden. Wenn man DDM mit nur wenigen Servern an einem Standort einsetzt, braucht man sich darüber keine großen Gedanken zu machen. Es bietet sich in diesem Fall an, einen Server für die Sammlung der Daten zu definieren, der Informationen von allen anderen Servern in der Domäne einsammelt.



Strukturiert: Über Sammlungshierarchien wird gesteuert, auf welchen Servern welche Ereignisse von welchen anderen Servern eingesammelt werden.

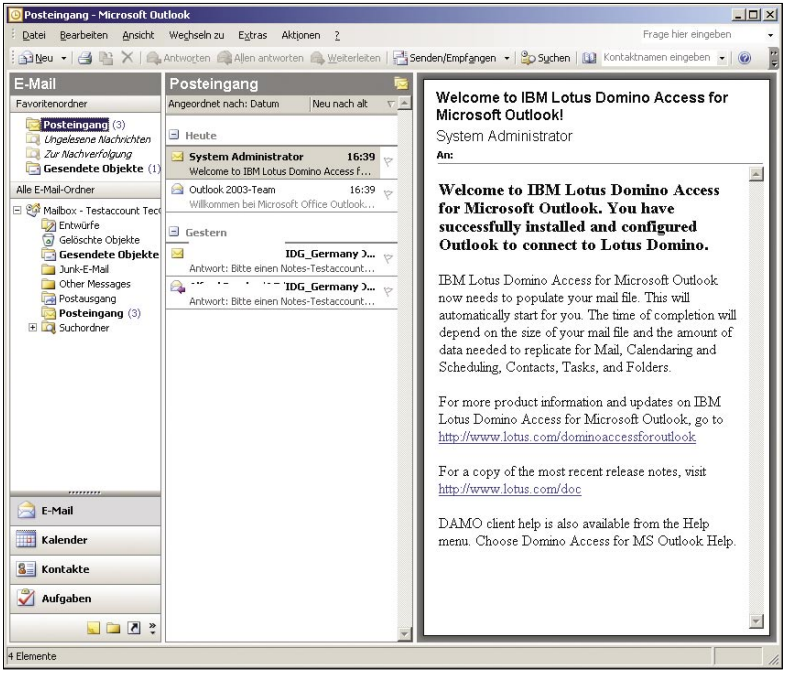
Hat man aber viele Server, die sich auch an anderen Standorten befinden, kann man manuell eine Hierarchie erstellen, in der festgelegt ist, welche gesammelten Informationen an welche Server weitergeleitet werden. Diese Hierarchie kann auch mehrstufig sein. Damit lassen sich etwa zunächst Daten von einem Standort konsolidieren und anschließend an einen zentralen Server weiterleiten. Hier gilt, wie in allen anderen Bereichen des DDM: Die Kunst liegt darin, einerseits die kritischen Situationen auf Servern zu erkennen und andererseits nicht zu viele Daten zu sammeln. Denn zum einen bedeutet jede Probe zusätzliche Last und zum anderen muss man die Ereignisse auch auswerten und erkannte Probleme lösen. Deshalb sollte man zunächst gründlich planen, wofür man DDM nutzen möchte, bevor man beispielsweise anfängt, alle vorkonfigurierten Probes zu aktivieren.

Martin Kuppinger

tecCHANNEL-Links zum Thema	Webcode	Compact
Domino Domain Monitoring richtig nutzen	460446	S.184

5.3 DAMO: Outlook und IBM Domino – elegant kombiniert

IBM und Microsoft sind beide große Player im Groupware-Bereich. Während Microsoft mit Exchange und Outlook aufwarten kann, setzt IBM Domino und Lotus Notes dagegen. Die Entscheidung für eine Lösung ist meist endgültig, denn ein Umschwenken auf das Konkurrenzsystem bedeutet Zeit- und Geldverlust. Somit ist auch der User selbst meist auf einen Client angewiesen.



Outlook statt Notes: Mit dem passenden Connector lassen sich beide Groupware-Lösungen problemlos verbinden.

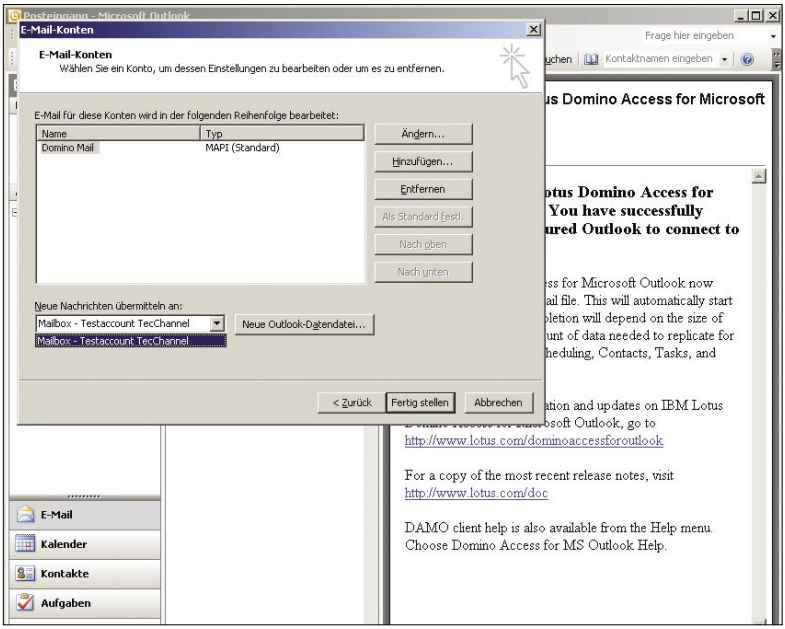
Während IBM mit Domino im Server-Bereich einen guten Job macht, kommt der Client Lotus Notes dagegen meist weniger gut weg. Zu umständlich, zu langsam, zu verschachtelt – in Benutzerkreisen wird Notes nicht gerade mit Lob überhäuft. Da scheint es gut ins Bild zu passen, dass IBM zur Notes-Lizenz auch einen Connector für Outlook mitliefert, den Domino Access for Microsoft Outlook, kurz DAMO. Wir haben uns die aktuelle Version 7.02 angesehen.

Bitte beachten Sie: DAMO 7.02 funktioniert nicht mit Outlook Express und Outlook 2007. Eine an Office 2007 angepasste Version ist bereits in Arbeit, sobald diese veröffentlicht wird, erfahren Sie das auf tecCHANNEL.de. Für den Test nutzten wir Outlook 2003, Lotus Notes 7.0.2 sowie Domino R 7.0.1FP1.

5.3.1 Die Technologie hinter DAMO

Entwickelt wurde der DAMO-Connector eigentlich, um Administratoren und Firmen einen Umstieg von Microsoft zu IBM zu ermöglichen. Hintergrund laut IBM: Während sich Administratoren und IT-Personal normalerweise relativ leicht an neue Arbeitsumgebungen gewöhnen, lösen gravierende Änderungen bei normalen Nutzern mitunter panikartige Zustände aus.

Um den Connector verstehen zu können, muss man zuerst die Unterschiede zwischen Exchange/Outlook und Domino/Notes kennen. Diese beginnen bereits bei der Speicherung der Dateien. Eine Exchange/Outlook-Umgebung sichert alle Dateien zentral in einer Exchange-Datenbank, denn die einzelnen PST-Dateien der Outlook-Installationen lassen sich nicht zentral vernetzen. Domino/Notes setzt auf das Replizierungsverfahren, bei dem nur jeweils die Änderungen zwischen Client- und Server-Datenbank übertragen werden.



Verständigung: DAMO schaltet sich als Vermittler zwischen Domino-Server und Outlook-Client.

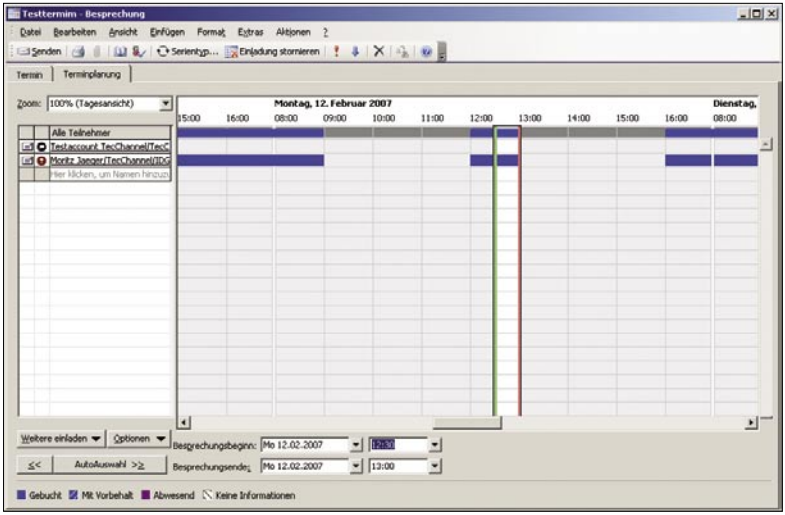
Outlook spricht mit Domino

Ein weiterer Unterschied und Hauptkritikpunkt an Exchange ist, dass Microsoft auf das proprietäre MAPI-Protokoll zur Datenübertragung setzt. Damit sperrt Microsoft die meisten Konkurrenten aus. Mit DAMO erstellt IBM nun einen virtuellen Tunnel für den Outlook-Client. Der Trick ist, dass alle Änderungen und Dateien sowohl im Domino-NSF-Dateisystem als auch in der lokalen Outlook-PST gespeichert werden. DAMO selbst repliziert dann neue Einträge nahezu sofort zwischen beiden Datenbanken.

Weder der Domino-Server noch der Notes- oder Outlook-Client werden bei der Prozedur verändert. Im Endeffekt stehen die Daten einfach sowohl lokal als auch auf Server-Seite zur Verfügung, der User bekommt davon nichts mit. Ein weiterer Vorteil von DAMO ist die freie Wahl des Clients. Sowohl Lotus Notes als auch Outlook haben jederzeit Zugriff auf die Dateien, somit steht immer eine Fall-Back-Lösung bereit, wenn Outlook ausfällt.

5.3.2 Terminplanung und Kontaktverwaltung

Neben der Hauptfunktion der Groupware-Clients, dem Schreiben und Empfangen von Mails, nehmen auch Kontaktverwaltung und Terminplanung einen wichtigen Teil der Funktionen ein. Die E-Mail-Übertragung lässt sich notfalls auch per Workaround, etwa per POP3 oder IMAP, realisieren, bei der zentralen Regelung von Adressdaten und Kalendereinträgen ist das aber nicht so ohne weiteres möglich.

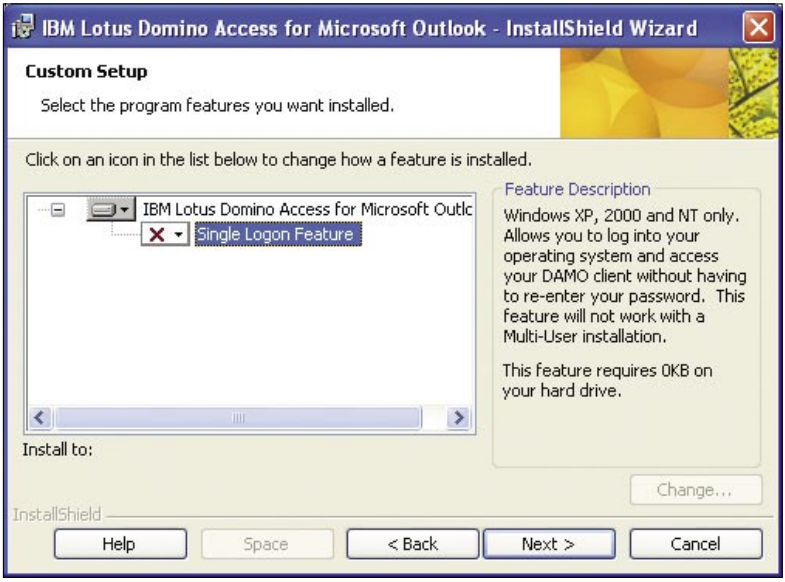


Verplant: Wenn Sie andere Nutzer einladen, können Sie sehen, ob diese bereits woanders verbucht sind.

Anders sieht es beim Einsatz von DAMO aus. Der Connector ermöglicht Outlook sowohl den Zugriff auf zentrale Adressbücher als auch auf die komplette Kalenderfunktion. Praktisch dabei: Auch in Outlook sieht der Nutzer, ob ein Gesprächspartner zur geplanten Zeit bereits auf einem Termin ist. Für die Kontaktverwaltung lässt DAMO den Outlook-Client wahlweise direkt auf das Online-Verzeichnis oder die lokalen Datenbanken zurückgreifen. Zudem lassen sich die Datenbanken vom Server auf das lokale System kopieren.

5.3.3 Workshop: Installation von DAMO

Die Installation des Connectors ist schnell erledigt. Das Installationspaket steht bei IBM unter www-128.ibm.com/developerworks/lotus/downloads/ zum Download bereit. Lassen Sie sich nicht von der Bezeichnung „Trial“ irritieren. Die Software ist keinerlei Einschränkungen unterworfen. Während der Installation können Sie entscheiden, ob DAMO in einer Single- oder Multi-User-Umgebung installiert werden soll. Der Unterschied: In Multi-User-Umgebungen können Sie für jeden Nutzer einen eigenen Ordner anlegen.



Single Sign-On: Das Feature erspart Ihnen die Passworteingabe in Outlook.

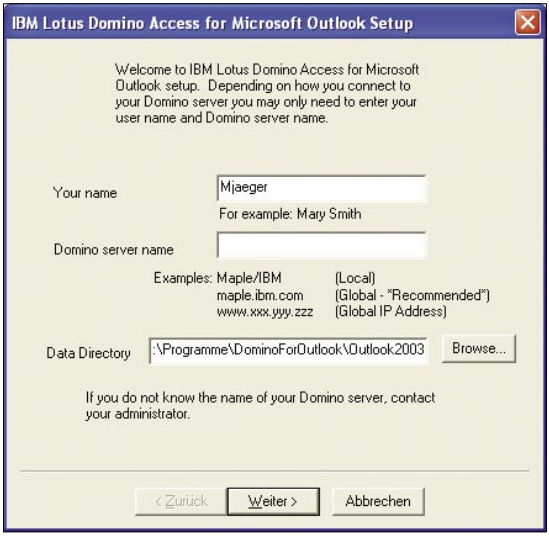
Auf Wunsch können Sie zusätzlich das Single-Sign-On-Paket einrichten. Das macht dann Sinn, wenn Ihr Benutzerkonto- und Ihr Notes-Passwort dasselbe ist. Haben Sie sich an Ihrem Windows-Account angemeldet, können Sie in Outlook

auf Ihre Mails zugreifen, ohne ein neues Passwort eingeben zu müssen. Damit ist die Installation des Connectors selbst abgeschlossen. Nun sollte automatisch der Assistent zum Einrichten der Konten starten. Geschieht dies nicht, wählen Sie im Windows-Startmenü den Eintrag „Create New MAPI Profile“.

5.3.4 Einrichten der Konten

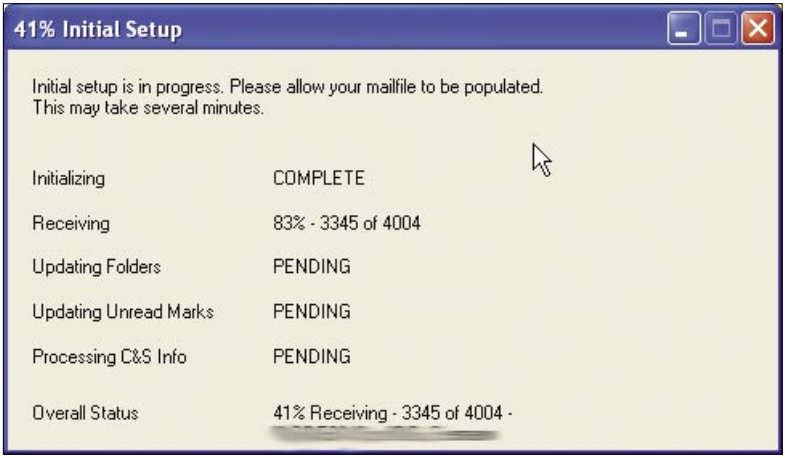
Um Outlook per DAMO mit Domino zu verbinden, benötigen Sie vier Angaben:

- Den Namen des Notes-Accounts
- Den Pfad zum Domino-Server
- Die Notes-ID-Datei
- Das Passwort



Grundangaben: Ohne Benutzername und Pfad zum Server geht in DAMO gar nichts.

Beenden Sie nun unbedingt jede laufende Notes-Instanz, die auf das Benutzerkonto zugreift. Tragen Sie den Namen des Kontos und den Server-Pfad in das erste Fenster des Assistenten ein. In Multi-User-Umgebungen können Sie außerdem einen Pfad für das Verzeichnis des Users eintragen. Sobald Sie auf „Weiter“ klicken, versucht sich DAMO mit dem Server zu verbinden und den Nutzer zu verifizieren. Nun sollte Sie der Assistent nach der passenden ID-Datei fragen, die er auf Wunsch auch gleich in das Verzeichnis des Nutzers kopiert. Geben Sie das Passwort für die Datei ein, klicken Sie auf „Fertig stellen“ im nächsten Fenster, und DAMO erstellt das neue MAPI-Profil.



Replizierung: Beim ersten Start gleicht der Server die Daten mit der lokalen PST-Datei ab.

Wenn keine Fehlermeldung auftaucht, war es das auch schon. Starten Sie Outlook, und Sie werden gefragt, welches Konto geöffnet werden soll. Wenn Sie sich das erste Mal an dem neuen Konto anmelden, müssen Sie per „Senden/Empfangen“ die Daten abgleichen. Je nach Postfachgröße kann das auch eine Weile dauern. Anschließend können Sie mit Outlook arbeiten.

5.3.5 Fazit

Mit DAMO hat es der Admin in der Hand, welchen Client er seinen Nutzern zur Verfügung stellt. Neben der Migration von einer Exchange- auf eine Domino-Umgebung kann man sich auch andere Einsatzgebiete für den Connector vorstellen. So flexibel und programmierbar Notes an sich ist, es strotzt nicht eben vor Usability. Teilweise ist auch der Einsatz auf betagten Rechnern mangels RAM oder CPU-Leistung nicht mehr produktiv möglich. Hier bietet sich ein Outlook-Einsatz geradezu an. Denn auch wenn Outlook oft in der Kritik steht, so ist es doch, gerade für technisch weniger versierte Nutzer, leichter zu verstehen. Ein weiteres Szenario könnte der Einsatz von Windows-Mobile-basierten Geräten sein, die sich nur schwer zur Synchronisation mit Domino/Notes überreden lassen.

Im Test beeindruckt vor allem die Geschwindigkeit des Connectors. Neue E-Mails oder Kalenderdaten landen nahezu ohne Verzögerung im Outlook-Postfach. IBM setzt mit der doppelten Datenbank wirklich einen cleveren Trick ein, der zudem die Hemmschwelle zum Testen senkt. Denn da die Notes-Datenbanken selbst unangetastet bleiben, kann man DAMO sogar „einfach mal so“ ausprobieren. Wenn es nicht klappt, hat man ja immer noch seine normale Notes-Installation, die von Änderungen nicht betroffen ist.

Das einzige Problem in unserem Test waren die zusätzlich programmierten Notes-Anwendungen, beispielsweise ein Planer für Raumbelegungen. Diese stehen unter Outlook nicht mehr zur Verfügung. Ansonsten blieb die Verbindung im Test stabil und flink. DAMO gibt es derzeit nur für Windows, Nutzer von Mac OS oder Linux gehen leer aus.

Moritz Jäger

tecCHANNEL-Links zum Thema	Webcode	Compact
DAMO: Outlook und IBM Domino – elegant kombiniert	460009	S.190
Domino: Der Server-basierte Zertifikatsdienst	460940	S.177
Domino Domain Monitoring richtig nutzen	460446	S.184
So funktioniert E-Mail	401772	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Suchfeld von www.tecChannel.de ein und wählen Sie „Webcode" als Suchbereich. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

Glossar

➥
Fortsetzung des Listings der vorangegangenen Zeile.

CGI

Common Gateway Interface. Definierte Schnittstelle, über die der Webserver externe Programme aufrufen und deren Ergebnisse als Webseiten zur Verfügung stellen kann.

Daemon

Ein Daemon lässt sich mit einem Dienst unter Windows NT vergleichen. Er stellt beispielsweise einen FTP- oder HTTP-Server zur Verfügung.

DHCP

Dynamic Host Configuration Protocol. Bei DHCP bezieht ein Arbeitsrechner seine Konfiguration des IP-Netzwerks von einem Server.

DMZ

Entmilitarisierte Zone, demilitarized zone: Dabei befinden sich Bastion-Host, Informations-Server, Modem-Pools sowie andere Server im DMZ-Netz.

DNS

Domain Name System (oder Service). Internet-Dienst, der Domain-Namen wie www.ibm.de in die zugehörigen IP-Adressen umsetzt.

DoS

Denial of Service. Hacker-Angriff auf einen Rechner, der den angegriffenen Computer lahm legt, so dass er auf Anfragen nicht mehr reagieren kann.

DSL

Digital Subscriber Line. Die Standleitung ins Internet für kleine Firmen und Privatpersonen. DSL arbeitet mit denselben Kupferkabeln wie analoge Telefone und ISDN-Anschlüsse.

FAQs

Frequently Asked Questions. Eine Liste häufig gestellter Fragen mit den dazugehörigen Antworten. FAQs werden von Herstellern und Anwendern zu zahlreichen Themen angeboten.

Firewall

Software zur Sicherung des LAN vor Angriffen aus dem Internet.

https

Protokollkennzeichner für über SSL gesicherte http-Verbindungen.

IANA

Internet Assigned Numbers Authority. Zeichnet für die Administration des Domain Name System (DNS) verantwortlich. Regelt über regionale Registrare die Vergabe von IP-Adressen und Top Level Domains (TLDs).

ICMP

Internet Control Message Protocol. TCP/IP-Protokoll zum Austausch von Fehler- und Statusmeldungen.

LDAP

Lightweight Directory Access Protocol. Standardisiertes Netzwerkprotokoll zum Zugriff auf Verzeichnisdienste, über die sich Ressourcen wie etwa E-Mail-Adressen finden lassen.

Masquerading / NAT

Network Address Translation. Bei NAT handelt es sich um ein Verfahren zur Abschottung des LAN gegenüber dem Internet. Dabei wird zum Internet hin immer nur die Adresse des Gateways gemeldet.

MD5

Beim dem Message-Digest-Algorithmus Version 5 handelt es sich um einen Verschlüsselungsalgorithmus, der vorwiegend zur Erzeugung digitaler Signaturen verwendet wird.

NFS

Network File System. Spezielles Dateisystem, das in Unix-Umgebungen den Zugriff auf entfernte Verzeichnisse und Dateien ermöglicht.

NIS

Network Information Services. Früher als Yellow Pages (YP) bezeichnet. Dient der Verteilung von wichtigen Daten (Passwörter, Adressen, Schlüssel-Codes) vom Server an den Client.

NOS

Network Operating System, Netzwerkbetriebssystem. Allgemeine Bezeichnung für Betriebssystem, das für den Server-Einsatz vorgesehen ist, wie zum Beispiel Novell Netware oder Windows NT Server.

PAM

Pluggable Authentication Modules. Bezeichnet mehrere Bibliotheken, die für Unix-Anwendungen gemeinsame Methoden zur Benutzerauthentifizierung zur Verfügung stellen. Neben der eigentlichen Authentifizierung stellen PAMs auch Methoden zur Behandlung von Benutzerkonten und Sitzungsdaten zur Verfügung.

PAP

Password Authentication Protocol. Bei PAP authentifiziert sich ein Einwahl-Client per Benutzernamen und Passwort beim Server.

POP / POP3

Post Office Protocol. Eines von zwei Standardprotokollen zur Zustellung von E-Mails an einen Mail User Agent. Alle gängigen E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server.

Port

Ein TCP-Port dient als Kommunikationskanal für den Zugriff auf einen Internet-Rechner über das TCP/IP-Protokoll, ähnlich den Nebenstellen eines Telefonanschlusses.

Index

A
Active Directory 163, 169
Administration Requests 182
ADSL 13
ASCII-Codierer 144
Ausfallsicherheit 125

B
BackTrack 84
Bayes-Filter 157
Benutzerdefinierte Tasks 173
Beowulf 47
Berechtigungen 174
Blockierlisten 149

C
CA-Prozes 177
cert.id 178
Certificate Authority Administrators 178
Certificate Requests 182
Certificate Revocation Lists 178, 182
Challenge-Response 155
Chirp Spread Spectrum 27
Clientfilter 160
Client Lifecycle Management 162
CloneXP 69
Cluster 42
Collaboration 55
Coyote Linux 86
Cron-Server 13

D
Damn Small Linux 84
DAMO 190
Data Grids 50
Data Warehouse 134
DBWn 135
DC 52
DDM Probes 186
Default Domain Controllers Policy 165
Default Domain Policy 165
Detection (NNIDS) 36
DHCP-Administratoren 170
Dienste 176
DIP-Schalter 12
Distributed Computing 42
Distributionen 83
Domain Monitoring 184
Domänen-Admins 170
Domino 177, 184, 190
Domino Access for Microsoft Outlook 190
Downtime 125

E
End Entities 179
EnOcean 29
Enterprise Manager 139
Enterprise Service Bus 112
Enterprise Volume Management System 100
Events 184
Exchange 191

F
Failover 46
Feather Linux 85
Fehlersituationen 185
Fli4l 86
Forest-Root-Domäne 169
Fritz!Box 10
Front-End-SMTP-Server 159
Funkbasierte Anwendungen 22

G
G4L 87
Gebäudeautomation 22
GeeXboX 87
GParted 88
GPMC 163
GPO 164
Grid 42
Grid Computing 48, 132
grml 89
Group Policy Management Console 163
Group Policy Objects 164
Groupware 190
Gruppenrichtlinien 162

H
High Availibility Cluster 44
High Performance Cluster 46
Hochverfügbarkeits-Cluster 44
Home Automation 22
HomeRF 27
Honeypot 31, 39
Horstbox 11
Host-based Intrusion Detection (HIDS) 34
Hub-and-Spoke 113

I
IDS 31
IEEE805.15 26
Information Grids 51
Internet Control Message Protocol 61
IPCop 90
IPS 31
IPsec over WLAN 13
ISM 22
Issued Certificate Lists 178, 182

J
Java Message Service 108

K
Kollaborationssoftware 177
Konten 194
Konten-Operatoren 171

L
Latenzzeit 43
LCOS 11
LDAP-Verzeichnis 172
Linux-Distributionen 83
Linux From Scratch 91
Live-CD 75
Load Balancing 46
Logical Volume Management 100
Lotus Notes Template Development 186

M
Machine-to-Machine-Communication 24
Majordomo 156
Managementstation 32
Meshing 23
Message Oriented Middleware 108
Monitoring 184
mountallfs 70
Multi-Hop-Topologien 23

N
NCP-Server 103
Network-based Intrusion Detection 32
Networked Computing 42
Network Node-based Intrusion 36
Notes 177
Novell 98
Novell Remote Manager 99
Novell Storage Services 98
NSF-Dateisystem 192
NSS Management Utility 101
Ntfsundeleteall 71
NTP-Server 13

O
OASIS 117
Objektklasse 174
Open Enterprise Server 98
Organisations-Admins 170
Outlook 145, 190

P
Packet Sniffing 58
Pattern Matching 37
Peer-to-Peer 42
Peer-to-Peer-Netzwerke 54
Performance-Planung 133
Ping 59
Probes 184
Protokollanalyse 37
Proxy 146
Punkt-zu-Punkt-Systeme 22
Puppy 75, 92

Q
QEMU 75

R
RAC-Architektur 133
Randfilter 159
Random-Back-Off-Algorithmus 28
Registration Agent 178
Relays 145
Remote Control 62

Repeater 24
Reverse-DNS-RBL-Dienste 151
RF-Transceiver 24
Richtlinien-Ersteller-Besitzer 170
ROKSO 147
Routing 24
RPC 110

S

S/MIME 177
Samba 72
Scalable Coherent Interface 43
Schema-Admins 170
Schichtenmodell 120
Self-Service-Portal 173
Sensoren 32
Server-ID 182
Server-Operatoren 171
Service Grids 50
Serviceorientierte Architekturen 105
Shared Computer Toolkit 63
Shared Memory 132
Signaturbasierte Filter 156
Single-Sign-On-Paket 193
SIP-Provider 13
Skalierbarkeit 133
Smarthost 159
SMTP 145
SMTP-Authentifizierung 13
SNMP-Traps 13
SOA 105
SOAP 117
Spam 144
Spamhaus Register of Known Spam Operations 147
Speicherfilter 160
SSH 14
SSL 177
Standardrichtlinien 165
System (NIDS 32
Systemausfälle 125
SystemRescueCD 93

T

Tasks 172
Telefonie-Funktionen 16
Telnet 14
TFTP 14
Tk-Anlage 10
Traffic-Monitoring 58
Trinity Rescue Kit 65

U

Überwachungsfunktionen 184
Überwachungssysteme 31
UDDI 108, 118
Ultra-Wide-Band 27

V

Verbindungsfilter 152
Viren 144
Virtualisierung 77
Voice over IP 10
VPN 16
VPN-Server 15

W

W3C 117
Web Service Description Language 107
Web Services 117
Web Services Stack 120
WLAN 24
Wolfpack 47
WPAN 26
WSDL 118

X

X.509v3 177
XScale 11

Z

Z-Wave 28
Zertifikate 177
ZigBee 27
Zugriffsberechtigungen 169